Routeur Telindus 1421 SHDSL

Routeur Telindus 1421 SHDSL

Manuel d'utilisation et de référence

Version: 1.0 - 196471

Telindus Technical Publications – Geldenaaksebaan 335 - B-3001 Leuven - Belgium – Tel. +32 16 382011

Caractéristiques de la documentation

Objet	Routeur Telindus 1421 SHDSL
Type de manuel	Manuel d'utilisation et de référence
Version	1.0
Code	196471
Date de modification	25 March 2005 ©Telindus

Note sur le copyright

Les informations et descriptions contenues dans la présente publication sont la propriété de Telindus. Ces informations et descriptions ne peuvent être copiées ni reproduites sous quelque forme que ce soit sans l'autorisation écrite préalable de Telindus.

Cette publication peut présenter certaines imprécisions ou inexactitudes techniques, ou des erreurs typographiques pour lesquelles Telindus ne saurait être tenue pour responsable. Des modifications sont régulièrement apportées aux informations présentées ici ; ces modifications seront incorporées dans la nouvelle édition de cette publication. Telindus se réserve le droit de procéder à des améliorations et/ou des changements sur les produits décrits dans cette documentation, sans préavis.

Exigences de sécurité

Lisez attentivement les instructions de sécurité au début de MU-2 - Installation et connexion de l' Routeur Telindus 1421 SHDSL page 10.

Les connecteurs du Routeur Telindus 1421 SHDSL ne doivent être raccordés qu'aux types de circuits suivants:

Nom du connecteur	Etiquette	Type de connecteur	Type de circuit
Connecteur LAN	LAN	RJ45	SELV
Connecteur de ligne SHDSL	LIGNE	RJ12	TNV-1
connecteur de contrôle	CTRL	subD-9	SELV

- SELV (Safety Extra Low Voltage): connexion locale (p. ex. PC à Routeur Telindus 1421 SHDSL) ou ligne louée à l'intérieur du bâtiment.
- TNV-1 (Telecom Network Voltage): Ligne louée à l'extérieur du bâtiment.
- TNV-2: PSTN du PABX à l'intérieur du bâtiment.
- TNV-3: PSTN du PABX opérateur à l'extérieur du bâtiment.

Déclarations

CE

www.telindusproducts.com → Telindus Access Solutions → Products → Choose a product → Downloads → Certificates

Hereby, Telindus declares that this Routeur Telindus 1421 SHDSL complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Hierbij verklaart Telindus dat deze Routeur Telindus 1421 SHDSL overeenstemt met de essentiële vereisten en andere relevante bepalingen van Richtlijn 1999/5/EC.

Par la présente, Telindus déclare que ce Routeur Telindus 1421 SHDSL est en conformité avec les exigences essentielles et autres articles applicables de la Directive 1999/5/CE.

Hiermit, Telindus erklärt daß dieser Routeur Telindus 1421 SHDSL in Fügsamkeit ist mit den wesentlichen Anforderungen und anderen relevanten Bereitstellungen von Direktive 1999/5/EC.

Mediante la presente, Telindus declara que el Routeur Telindus 1421 SHDSL cumple con los requisitos esenciales y las demás prescripciones relevantes de la Directiva 1999/5/CE.

A Telindus declara que o Routeur Telindus 1421 SHDSL cumpre os principais requisitos e outras disposições da Directiva 1999/5/EC.

Col presente, Telindus dichiara che questo Routeur Telindus 1421 SHDSL è in acquiescenza coi requisiti essenziali e stipulazioni attinenti ed altre di Direttivo 1999/5/EC.

Με το παρόν η Telindus δηλώνει ότι το Routeur Telindus 1421 SHDSL είναι συμμορφούμενο με τις βασικές απαιτήσεις και με τις υπόλοιπες σχετικές διατάξεις της οδηγίας 1999/5/EC.

Documentation du Routeur Telindus 1421 SHDSL

La documentation du Routeur Telindus 1421 SHDSL se compose actuellement des documents suivants:

Document	Description
Routeur Telindus 1421 SHDSL Manuel (ce manuel)	Il s'agit du manuel que vous avez actuellement entre les mains. Il vous indique comment installer et raccorder le Routeur Telindus 1421 SHDSL et vous présente une configuration de base. Il contient également une description complète de tous les paramètres de configuration, d'état, de performance et d'alarme, à des fins de consultation.
manuels d'application de maintenance et de gestion	Le Routeur Telindus 1421 SHDSL peut être entretenu et géré par un grand nombre d'outils de maintenance et de gestion. Reportez-vous à MU-1.3 - Outils de gestion et de maintenance page 7 pour une présentation de ces outils et obtenir la référence du manuel de ces outils.
documents sur câbles	Il existe une grande variété de câbles permettant de connecter le Routeur Telindus 1421 SHDSL. Le document intitulé Câbles de données (PDF) et le document Câbles de commande (PDF) décrivent ces divers types de câbles.

Tous ces documents, ainsi que l'outil de maintenance gratuit TMA et le firmware des unités Telindus se trouvent sur le CD Produits d'Accès Telindus qui est fourni avec tous les produits Telindus.

Organisation de ce manuel

Ce manuel se compose de trois parties:

Pièce	Cette partie…
Manuel d'utilisation	vous indique comment installer et raccorder le Routeur Telindus 1421 SHDSL. Il vous propose également une configuration de base du Routeur Telindus 1421 SHDSL. Cette partie est en français.
Manuel de référence	donne des informations plus détaillées sur le Routeur Telindus 1421 SHDSL, comme, par exemple, la procédure de téléchargement du logiciel, les spécifications techniques, etc. Il contient également une description complète de tous les paramètres de configuration, d'état, de performance et d'alarme, à des fins de consultation. Cette partie est en anglais.
Annex	donne des informations complémentaires, par exemple les codes de vente des produits. Cette partie est en anglais.

Conventions typographiques

Les conventions typographiques suivantes sont utilisées dans ce manuel:

Le format …	indique …
Normal	le texte normal.
Italic	• les mots nouveaux ou qui doivent ressortir • fenêtre, boutons et champs d'application, par exemple dans le champ *Fichier* nom entrée …
`Computer`	texte que vous devez entrer lors de l'invite DOS ou CLI, exemples de sortie ordinateur et code. P. ex. `NOK,1,1,Invalid command.`

`Computer Bold`	texte que vous devez entrer lors de l'invite DOS ou CLI lorsqu'il s'agit d'un mélange d'entrées et de sorties d'ordinateur.
	P. ex.
	`/o1003:"Edit Configuration"`
	`>`**`get sysName`**
	`  sysName = "Orchid 1003 LAN"`
	`/o1003:"Edit Configuration"`
	`>`

Narrow	les objets et attributs de l'arborescence d'une unité lorsqu'ils sont mentionnés dans le texte normal. Par exemple, lorsqu'ils ne font pas partie d'une entrée ou d'une sortie ordinateur. P. ex. utilisez l'attribut sysName pour …
<Narrow>	objets ou attributs de l'arborescence, ou parties d'entre eux, qui sont variables. Par exemple, en fonction de la version du produit, de l'interface utilisée, etc., les noms de ces objets et attributs peuvent différer légèrement. P. ex. topObject/<modularIf>/someAttribute signifie que le nom de l'objet <modularIf> dépend de l'interface modulaire que vous utilisez. Par exemple, v35 avec une interface V.35, g703 avec une interface G.703, etc.
Blue	références à d'autres parties de ce manuel. P. ex. “Refer to xx - Title pour de plus amples informations ”.
Soulignement bleu	• hyperlien à un site web. P. ex. www.telindus.com • référence à un autre manuel. P. ex. “Reportez-vous au manuel TMA (PDF) pour de plus amples informations ”. Les abréviations entre guillemets indiquent le format du fichier (PDF = Portable Document Format / CHM = Compiled HTML Help).

Conventions graphiques

Les icones suivants sont utilisés dans ce manuel:

Icone	Nom	Cet icone indique …
	Remarque	remarques ou conseils utiles.
	Avertissement	texte à lire attentivement pour éviter tout dommage à l'appareil.
	Alerte	texte à lire attentivement pour éviter toute blessure.
	DIP switch	commutateur DIP ou tableau de barrettes.
	Attribut de base	attribut de base dans l'arborescence du Routeur Telindus 1421 SHDSL.
	Attribut avancé	attribut avancé dans l'arborescence du Routeur Telindus 1421 SHDSL.
	Attribut de structure	attribut structuré au sein d'un autre attribut dans l'arborescence du Routeur Telindus 1421 SHDSL.
	Action	action dans l'arborescence du Routeur Telindus 1421 SHDSL.

Lecture d'un tableau de commutation DIP

Des tableaux de commutateurs DIP sont présentés en différents endroits de ce manuel. Pour vous permettre de lire ces tableaux, lire ce qui suit.

Un tableau de configuration de commutateurs DIP se présente de la façon suivante:

DIP switch name	DS1 no.	Setting	Funtion
	1	**on**	
		off	

1 2 3 4 5

Le tableau suivant explique la structure du tableau de configuration de commutateurs DIP.

Numéro	Cette position affiche…
1	L'icone du commutateur DIP.
2	Le nom du commutateur DIP.
3	la position du commutateur DIP dans la banque de commutateurs DIP. Les abréviations ont la signification suivante: DS1 no. 1: Banque de commutateurs DIP numéro 1, position de commutateur numéro 1
4	Possibilités de réglage du commutateur DIP: on et off. Le réglage par défaut est imprimé en gras.
5	La fonction associée au réglage du commutateur DIP correspondant.

Lecture d'une chaîne d'attributs

Des chaînes d'attributs sont présentées en différents endroits de ce manuel. Pour vous permettre de lire correctement ces chaînes, lire ce qui suit.

Une chaîne d'attributs se présente de la façon suivante:

tobObjectName/objectName/attributeName

Default: defaultValue
Range: valueRange

1 2 3

Le tableau suivant explique la structure de la chaîne d'attributs.

Numéro	Cette position affiche…
1	l'icone d'attributs. Il indique que la chaîne qui suit est une chaîne d'attributs. Reportez-vous à Conventions graphiques page vi pour de plus amples informations.
2	Le nom de l'attribut et sa position dans l'arborescence.
3	La valeur par défaut d'un attribut de configuration.

Version TDRE

le Telindus Dynamic Routing Engine (TDRE) est un système d'exploitation très riche en fonctions qui garantit un ensemble de caractéristiques communes sur toute la ligne de produits Telindus et une assistance uniforme par les outils de maintenance et de gestion.

Ce manuel décrit les caractéristiques, l'arborescence et les attributs du TDRE version 11.000.000.

Audience

Ce manuel est destiné aux personnes disposant de solides connaissances en informatique et en principes de réseau.

Vos réactions

Votre satisfaction quant à cet achat constitue l'une de nos principales priorités chez Telindus. En conséquence, tous les aspects électroniques, fonctionnels et esthétiques de cette nouvelle unité ont fait l'objet de tests et d'inspections soignés et approfondis. Si une défaillance quelconque est constatée sur cette unité ou si vous avez des commentaires relatifs à la qualité de la livraison, veuillez remplir le Formulaire de Commentaire de Qualité qui se trouve sur notre site web à l'adresse www.telindusproducts.com/quality.

Manuel d’utilisation

Routeur Telindus 1421 SHDSL

Manuel d’utilisation

Version: 1.0 - 196471

Telindus Technical Publications – Geldenaaksebaan 335 - B-3001 Leuven - Belgium – Tel. +32 16 382011

Table des matières

MU-1Présentation du Routeur Telindus 1421 SHDSL....4
MU-1.1Qu'est-ce que le Routeur Telindus 1421 SHDSL? 5
MU-1.2Routeur Telindus 1421 SHDSL applications 6
MU-1.3Outils de gestion et de maintenance 7
MU-1.4Possibilités de connexion des outils de gestion et de maintenance 9

MU-2Installation et connexion de l' Routeur Telindus 1421 SHDSL 10
MU-2.1Instructions de sécurité 11
MU-2.2Déballage 12
MU-2.3Sélection d'un emplacement 13
MU-2.4Montage mural du Routeur Telindus 1421 SHDSL 14
MU-2.5Installation et précautions de connexion 16
MU-2.6Connexion Routeur Telindus 1421 SHDSL 17
MU-2.7Témoins à DEL du panneau avant 21

MU-3Commutateurs DIP du Routeur Telindus 1421 SHDSL....26
MU-3.1La carte mère du Routeur Telindus 1421 SHDSL 27
MU-3.2Commutateurs DIP du Routeur Telindus 1421 SHDSL 28
MU-3.3Ouverture et fermeture du boîtier 29

MU-4Maintenance du Routeur Telindus 1421 SHDSL....30
MU-4.1Maintenance du Routeur Telindus 1421 SHDSL avec TMA 31
MU-4.2Introduction à la terminologie de gestion 37
MU-4.3Les objets dans l'arborescence Routeur Telindus 1421 SHDSL 41
MU-4.4Ajout d'un objet dans l'arborescence 43
MU-4.5Routeur Telindus 1421 SHDSL aperçu des attributs 48

MU-5Configuration de base 50
MU-5.1Qu'est-ce qu'une interface? 51
MU-5.2Configuration d'adresses IP 52
MU-5.3Configuration de la ligne SHDSL 64
MU-5.4Configuration des mots de passe 74
MU-5.5Exécution des actions de configuration 76
MU-5.6Configuration des principales fonctions du Routeur Telindus 1421 SHDSL 80
MU-5.7Dépistage des erreurs Routeur Telindus 1421 SHDSL 81

MU-6Configuration des protocoles d'encapsulation 82
MU-6.1Sélection d'un protocole d'encapsulation 83
MU-6.2Configuration d'encapsulation ATM 84
MU-6.3Configuration d'encapsulation de Frame Relay 105
MU-6.4Configuration d'encapsulation PPP 121
MU-6.5Configuration d'encapsulation HDLC 144
MU-6.6Configuration d'un test d'erreur 146

MU-7Configuration d'acheminement.....148
MU-7.1Introduction à l'acheminement..... 149
MU-7.2Activation de l'acheminement sur une interface 151
MU-7.3Configuration de chemins statiques..... 152
MU-7.4Configuration d'acheminement en fonction de la politique 161
MU-7.5Configuration de RIP 166
MU-7.6Configuration OSPF..... 177
MU-7.7Configuration de translation d'adresses..... 185
MU-7.8Configuration de la politique de trafic et de priorité sur le routeur 204

MU-8Configuration du pontage 224
MU-8.1Introduction au pontage..... 225
MU-8.2Configuration du pontage 236
MU-8.3Configuration de la politique de trafic et de priorité sur le pont..... 247

MU-9Configuration des fonctions complémentaires.....252
MU-9.1Configuration de DHCP 253
MU-9.2Configuration des restrictions d'accès 258
MU-9.3Configurer les VLAN 271
MU-9.4Configuration de tunnels L2TP 278
MU-9.5Configuration d'une sécurité IP..... 285
MU-9.6Configuration RADIUS..... 291
MU-9.7Configuration QoS 297

MU-10Exemples de configuration 308
MU-10.1Extension LAN par un réseau PDH/SDH..... 309
MU-10.2Extension LAN par un réseau à Frame Relay 311
MU-10.3Extension LAN par un réseau ATM 313
MU-10.4Connexion d'un LAN à l'internet en utilisant NAT et PAT 315
MU-10.5Utilisation de PAT avec un minimum d'adresses IP officielles..... 317
MU-10.6Combinaison de pontage et d'acheminement dans un réseau..... 319
MU-10.7Connexion de deux réseaux par un tunnel 321
MU-10.8Connexion de commutateurs à activation VLAN par un WAN..... 324
MU-10.9Multiplexage VLAN 326
MU-10.10Utilisation des listes d'accès étendu 329

Index..... 332

MU-1 Présentation du Routeur Telindus 1421 SHDSL

Ce chapitre présente le Routeur Telindus 1421 SHDSL. Le tableau suivant donne un aperçu de ce chapitre:

- MU-1.1 - Qu'est-ce que le Routeur Telindus 1421 SHDSL? page 5
- MU-1.2 - Routeur Telindus 1421 SHDSL applications page 6
- MU-1.3 - Outils de gestion et de maintenance page 7
- MU-1.4 - Possibilités de connexion des outils de gestion et de maintenance page 9

MU-1.1 Qu'est-ce que le Routeur Telindus 1421 SHDSL?

Le Routeur Telindus 1421 SHDSL est un modem professionnel du dernier cri à bande de base à routeur IP et pont intégré assurant une transmission symétrique en duplex intégral pouvant atteindre 2,3 Mbps par le biais d'un seul câble non blindé à paires torsadées et à deux conducteurs.

Le Routeur Telindus 1421 SHDSL peut être utilisé comme CPE en liaison avec des DSLAM et des IMAP ATM, Frame Relay ou PPP, ou en configuration point par point. Alors que les connexions ADSL asymétriques sont typiquement utilisées pour un accès résidentiel, le Routeur Telindus 1421 SHDSL est l'unité d'accès idéale pour la connexion d'utilisateurs professionnels, assurant des services de transmission symétriques gérés aux vitesses les plus élevées.

La vitesse de ligne peut s'adapter automatiquement pour optimiser le débit en fonction des caractéristiques de la boucle locale. Pour parvenir à des vitesses encore plus élevées (jusqu'à 4,6 Mbps) ou à une portée plus grande, une version à 2 paires de lignes est disponible.

Le Routeur Telindus 1421 SHDSL supporte des services différenciés basés sur des VPN (réseaux privés virtuels). Il intègre donc des fonctions telles que L2TP (Layer 2 Tunnelling Protocol), IPSEC, 802.1Q (VLAN tagging) et QoS (Quality of Service) basées sur Diffserv. Vous pouvez de plus procéder à un cryptage DES et 3DES. Un modèle spécifique supportant un accélérateur matériel pour le cryptage DES et 3DES est également disponible.

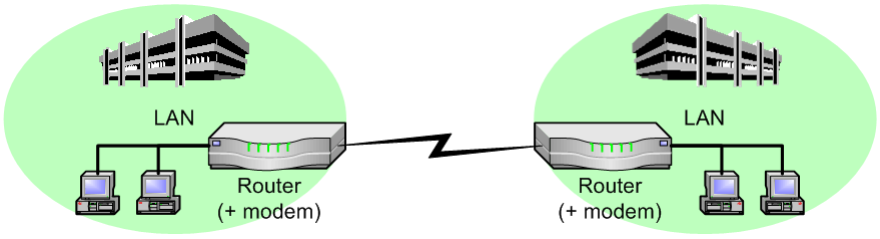
Le Routeur Telindus 1421 SHDSL est conçu pour être intégré dans des environnements réseaux très exigeants et peut être commandé par l'ensemble des outils de maintenance et de gestion de réseau. Il supporte des fonctions d'installation automatique par le biais du réseau WAN. Cela en fait le système idéal pour une installation de type plug-and-play dans les locaux des clients, et la configuration est prévue dans un site central.

MU-1.2 Routeur Telindus 1421 SHDSL applications

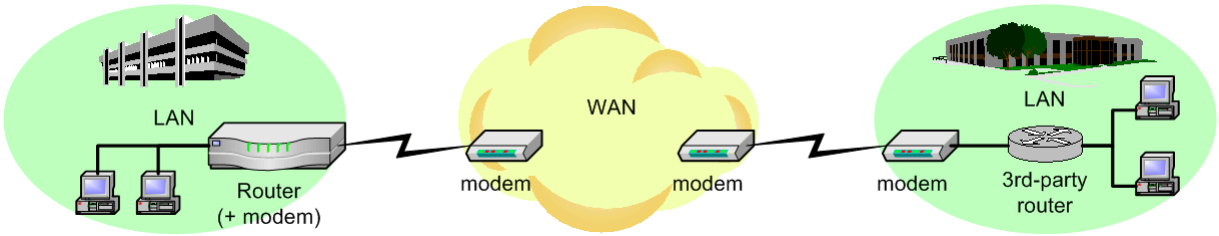
Exemples d'applications Routeur Telindus 1421 SHDSL:

- connexion LAN à LAN par le biais d'une ligne
- extension LAN par un réseau
- connexion LAN à internet

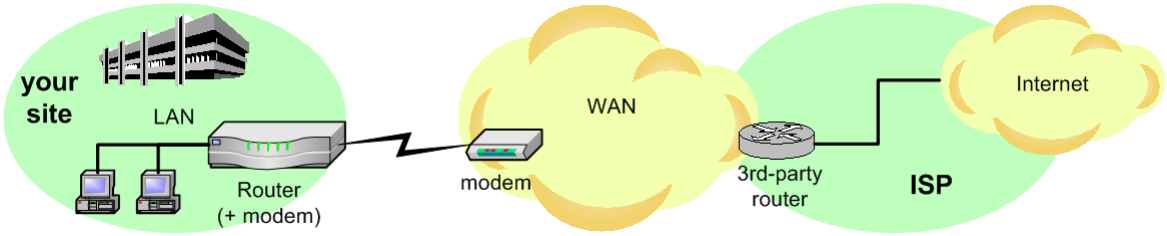
interconnexion LAN point à point



extension LAN par un réseau



connexion LAN à internet



MU-1.3 Outils de gestion et de maintenance

Le Routeur Telindus 1421 SHDSL peut être géré de différentes manières. Cette section donne un aperçu rapide des divers outils de gestion et de maintenance.

Outil de maintenance ou de gestion	Description et référence
TMA	TMA (application de maintenance Telindus) est un progiciel Windows libre disposant d'une interface utilisateur graphique qui vous permet de commander intégralement les produits Telindus, c'est-à-dire d'accéder à leurs attributs de configuration et d'observer leurs informations d'état, de performance et d'alarme. Reportez-vous à MU-4 - Maintenance du Routeur Telindus 1421 SHDSL page 30 et au manuel TMA (PDF) pour de plus amples informations.
Gestion d'éléments TMA	La gestion des éléments TMA est une application de gestion conçue pour contrôler un grand nombre d'unités Telindus. Il combine l'interface utilisateur graphique conviviale de la version autonome de la TMA avec une application d'enregistrement des événements appelée Element Viewer. Reportez-vous au manuel de gestion des éléments TMA (PDF/CHM) pour de plus amples informations.
TMA pour HP OpenView	TMA pour HP OpenView est l'application de gestion qui tourne sur la plate-forme de gestion de réseau largement répandue HP OpenView. Elle combine l'interface utilisateur graphique conviviale de la version autonome de la TMA avec les avantages et les fonctions de HP OpenView. Reportez-vous au manuel TMA pour HP OpenView (PDF) pour de plus amples informations.
TMA CLI	TMA CLI (TMA Command Line Interface) vous permet d'utiliser ses commandes en scripts pour automatiser les actions de gestion. Cela s'avère particulièrement utile dans le cas de grands réseaux. TMA CLI est un produit complémentaire de TMA, TMA Element Management et TMA pour HP OpenView. Reportez-vous au manuel TMA CLI (PDF) pour de plus amples informations.
ATWIN	ATWIN est une interface utilisateur à commande par menu. Vous pouvez lire et modifier tous les attributs comme avec la TMA, mais selon une représentation textuelle plus basique en utilisant un terminal VT100. Reportez-vous au manuel des outils de maintenance (PDF) pour de plus amples informations.
CLI	CLI est également une interface de ligne de commande, bien qu'elle ne soit pas si complète que TMA CLI. Les utilisateurs expérimentés, habitués à la syntaxe, peuvent accéder aux unités Telindus plus rapidement qu'avec TMA ou ATWIN. Reportez-vous au manuel des outils de maintenance (PDF) pour de plus amples informations.

Outil de maintenance ou de gestion	Description et référence
Interface web	L'interface web est une interface utilisateur commandée par un menu, de même type que ATWIN. Vous pouvez lire et modifier tous les attributs comme avec la TMA, mais selon une représentation textuelle plus basique en utilisant un navigateur web. Reportez-vous au manuel des outils de maintenance (PDF) pour de plus amples informations.
Borne EasyConnect	Connecter le terminal portable Telindus EasyConnect par le biais du connecteur de commande au Routeur Telindus 1421 SHDSL vous permet de gérer le Routeur Telindus 1421 SHDSL de manière basique en utilisant l'écran LCD et le clavier. Nous appelons ce type de commande la gestion depuis le clavier. Reportez-vous au manuel EasyConnect (PDF) pour de plus amples informations.
SNMP	Vous pouvez gérer le Routeur Telindus 1421 SHDSL par le biais de SNMP en utilisant n'importe quel navigateur SNMP. Le Routeur Telindus 1421 SHDSL supporte MIB2 et un MIB privé, y compris les circuits réjecteurs. Le MIB privé dispose de votre copie de TMA. Après l'installation des fichiers de données TMA, le fichier MIB privé est disponible dans le répertoire *C:\Program Files\TMA\snmp*[1] sous le nom *<filename>.mib*[2]. Reportez-vous à MR-1.12 - SNMP configuration attributes page 156 et à la documentation de votre navigateur SNMP pour de plus amples informations.

1. La première partie de ce chemin de répertoire peut être différente si vous n'avez pas choisi le trajet par défaut lors de l'installation des fichiers de données TMA.
2. Le nom du fichier est fonction du produit. Pour déterminer quel fichier MIB correspond à tel ou tel produit, reportez-vous au fichier *models.nms* (situé dans *C:\Program Files\TMA\model*[1]).

MU-1.4 Possibilités de connexion des outils de gestion et de maintenance

Le tableau qui suit donne un aperçu de tous les outils de maintenance et de gestion que vous pouvez connecter au Routeur Telindus 1421 SHDSL:

Outil de maintenance ou de gestion	**Connexion outil - Routeur Telindus 1421 SHDSL**		**Connexion outil – concentrateur de gestion[1]**	
	Série[2]	**IP[3]**	**Série[2]**	**IP[3]**
EasyConnect	**X**		**X**	
CLI	**X[4]**	**X[5]**	**X[4]**	**X[5]**
ATWIN	**X[4]**	**X[5]**	**X[4]**	**X[5]**
TMA	**X**	**X**	**X**	**X**
TMA CLI	**X**	**X**	**X**	**X**
Gestion d'éléments TMA		**X**		**X**
TMA pour HP OpenView		**X**		**X**
SNMP[6]		**X**		**X**
Interface web[7]		**X**		**X**

1. Des exemples de concentrateurs de gestion sont l'Orchid 1003 LAN, la série de routeurs Telindus 1030, la série Telindus 2300 SHDSL, etc. Reportez-vous à leurs manuels correspondants pour de plus amples informations sur la manière de régler ces unités comme proxy de gestion.
2. Une connexion série est une connexion entre le port COM de votre PC et le connecteur de commande du modem Crocus Routeur Telindus 1421 SHDSL utilisant un câble mâle-femelle DB9.
3. Une connexion IP est une connexion entre votre PC et le Routeur Telindus 1421 SHDSL par le biais d'un réseau IP.
4. Utilisation d'un terminal VT100 (programme d'émulation).
5. En utilisant Telnet.
6. En utilisant un navigateur SNMP.
7. En utilisant un navigateur web.

MU-2 Installation et connexion de l' Routeur Telindus 1421 SHDSL

Ce chapitre donne premièrement quelques instructions de sécurité importantes. vous indique comment installer et raccorder le Routeur Telindus 1421 SHDSL.

Il vous est conseillé de lire ce chapitre de manière séquentielle, du début à la fin, sans omettre aucune partie. Ce faisant, votre Routeur Telindus 1421 SHDSL sera entièrement installé et prêt à être configuré lorsque vous parviendrez à la fin de chapitre.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-2.1 - Instructions de sécurité page 11
- MU-2.2 - Déballage page 12
- MU-2.3 - Sélection d'un emplacement page 13
- MU-2.4 - Montage mural du Routeur Telindus 1421 SHDSL page 14
- MU-2.5 - Installation et précautions de connexion page 16
- MU-2.6 - Connexion Routeur Telindus 1421 SHDSL page 17
- MU-2.7 - Témoins à DEL du panneau avant page 21

MU-2.1 Instructions de sécurité

INSTRUCTIONS DE SECURITE IMPORTANTES

Déconnectez l'alimentation avant d'installer, de régler ou d'entretenir l'appareil.

AVERTISSEMENT DE SECURITE

Pour éviter tout dommage à l'équipement, veuillez respecter l'ensemble des procédures décrites dans ce chapitre.

Veillez à ce que l'unité et l'équipement connecté utilisent la même puissance CA et la même terre, pour réduire les interférences de bruit et les éventuels risques pour la sécurité causés par les différences de potentiels de terre.

MU-2.2 Déballage

Vérification du carton d'expédition

Une manutention sans précaution lors de l'expédition est la plupart de temps à l'origine des défaillances. Avant l'installation, vérifiez que le carton d'expédition ne présente aucun signe de détérioration:

- Si le carton est endommagé, signalez-le immédiatement au transporteur.
- Si le carton d'expédition ne présente aucune détérioration, ne le jetez pas et conservez-le pour stocker l'unité ou la renvoyer ultérieurement.

Contenu de l'emballage

Le carton doit contenir les articles suivants:

- Routeur Telindus 1421 SHDSL
- TMA CD-ROM (y compris ce manuel utilisateur et de référence en format PDF)

En option (selon les articles commandés):

- Alimentation externe avec cordon d'alimentation

MU-2.3 Sélection d'un emplacement

AVERTISSEMENT

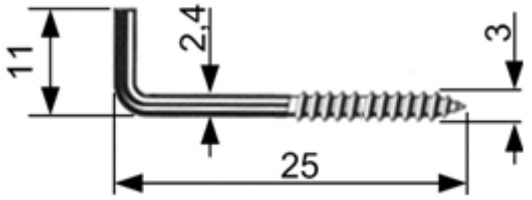
Placez toujours l'unité sur ses pieds, en veillant à ne pas bloquer les aérations.

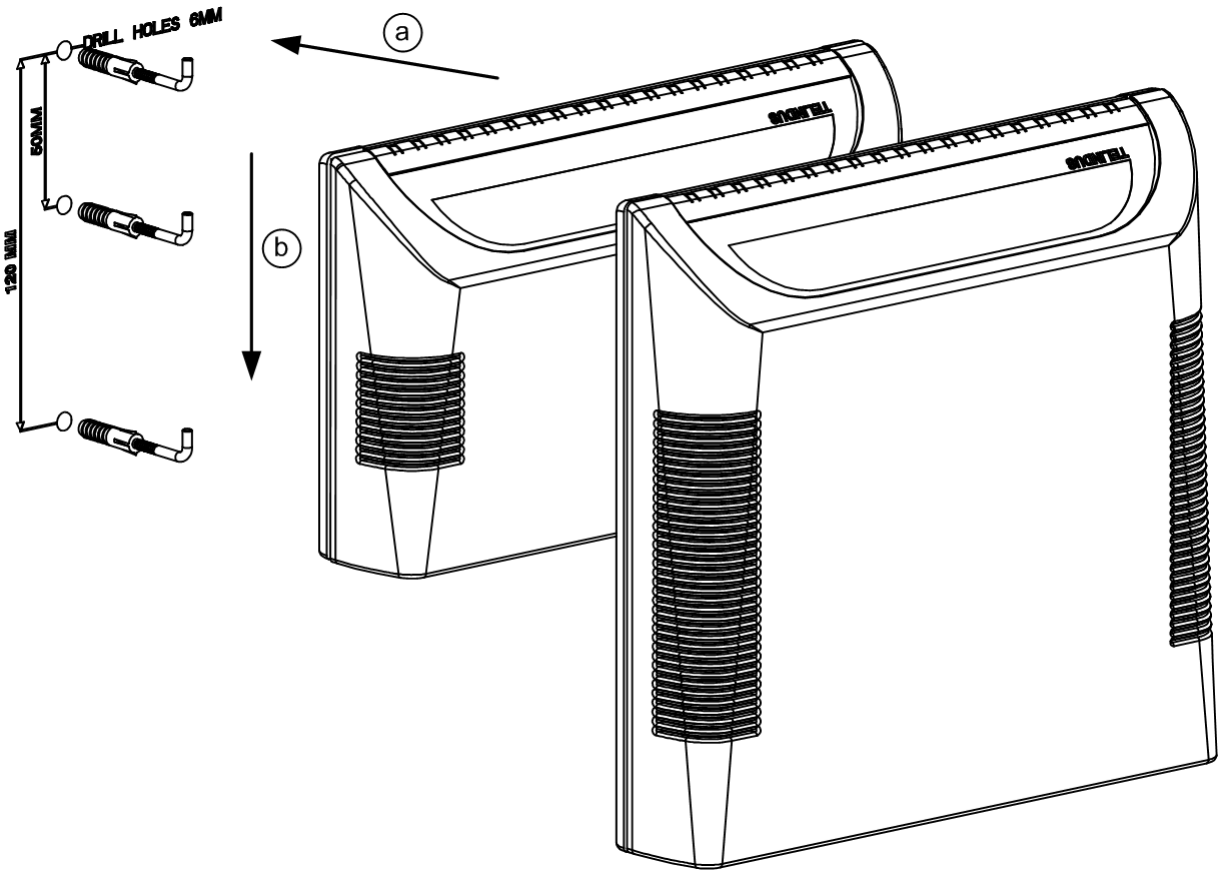
N'empilez pas plusieurs unités directement les unes sur les autres, cela pourrait entraîner une surchauffe qui endommagerait le matériel.

Installez l'unité dans un local non exposé à des températures extrêmes, à l'humidité, aux chocs et aux vibrations. Positionnez-la de manière à pouvoir facilement voir et accéder au panneau avant et à ses témoins de contrôle. Laissez un jeu suffisant à l'arrière pour les câbles et les fils. Positionnez l'unité de manière à garantir un accès adéquat aux différents raccordements et à deux mètres au maximum de la prise de courant.

MU-2.4 Montage mural du Routeur Telindus 1421 SHDSL

Le Routeur Telindus 1421 SHDSL peut être fixé au mur. Pour ce faire, procédez de la façon suivante:

Etape	Action
1	Forez deux trous dans le mur, en respectant les spécifications suivantes: • diamètre de forage 4 mm • distance entre les trous: - dans le cas du boîtier PBOX05: 120 mm - dans le cas du boîtier PBOX06: 60 mm • profondeur de trou au moins 25 mm
2	Insérez deux fiches murales dans les trous. Les fiches doivent avoir les dimensions suivantes: • diamètre: 4 mm • longueur: 20 mm
3	Vissez deux crochets carrés (plaque d'acier zingué et epox blanc) dans les fiches. Les crochets carrés doivent avoir les dimensions suivantes: 
4	Faites coulisser le Routeur Telindus 1421 SHDSL sur les crochets jusqu'à ce qu'il touche le mur, comme le montre la figure ci-dessous.
5	Faites coulisser le Routeur Telindus 1421 SHDSL vers le bas jusqu'à ce qu'il soit fermement fixé, comme le montre la figure ci-dessous.


DRILL HOLES 6MM
50MM
120 MM
a
b
ALCATEL
ALCATEL

MU-2.5 Installation et précautions de connexion

AVERTISSEMENT ESD

Les cartes de circuit sont sensibles aux décharges électrostatiques (ESD) et doivent être traitées avec soin. Il est recommandé d'assurer un contact électrique optimal entre vous-même, la zone de travail et une terre de sécurité avant de manipuler une carte de circuit. Veillez tout spécialement à ne toucher aucun composant ni aucun connecteur sur la carte de circuit.

AVERTISSEMENT EMC

Installation compatible EMC

Les produits d'accès Telindus sont compatibles EMC. Pour assurer la conformité avec la directive EMC 89/336/EEC, il convient d'utiliser des câbles blindés ou des perles de ferrite.

REMARQUE

Cet équipement peut être alimenté par un système d'alimentation IT.

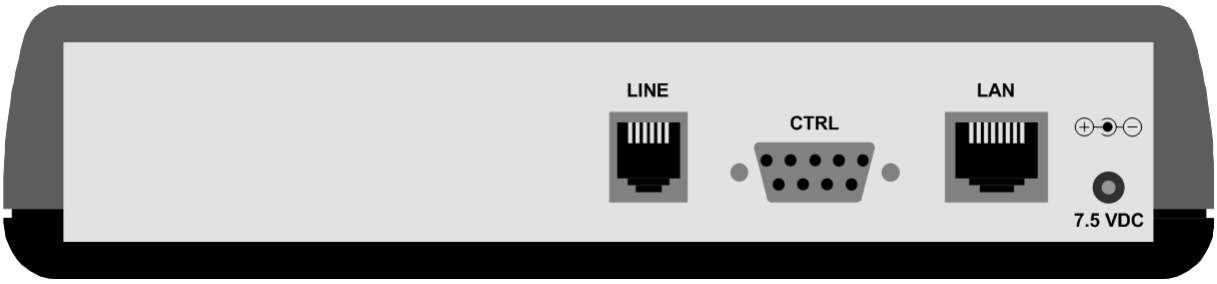
MU-2.6 Connexion Routeur Telindus 1421 SHDSL

Cette section explique comment connecter le Routeur Telindus 1421 SHDSL. Le tableau suivant donne un aperçu de ce chapitre:

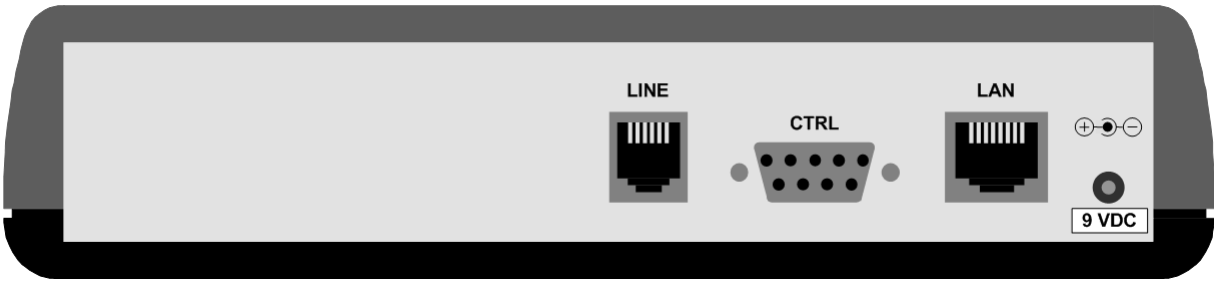
- MU-2.6.1 - Vue arrière du Routeur Telindus 1421 SHDSL page 18
- MU-2.6.2 - Connexion des différentes parties du Routeur Telindus 1421 SHDSL page 19
- MU-2.6.3 - Connexion du Routeur Telindus 1421 SHDSL - exemple page 20

MU-2.6.1 Vue arrière du Routeur Telindus 1421 SHDSL

La figure qui suit montre la face arrière du Routeur Telindus 1421 SHDSL 1P (1 pair):



La figure qui suit montre la face arrière du Routeur Telindus 1421 SHDSL 2P (2 pair):



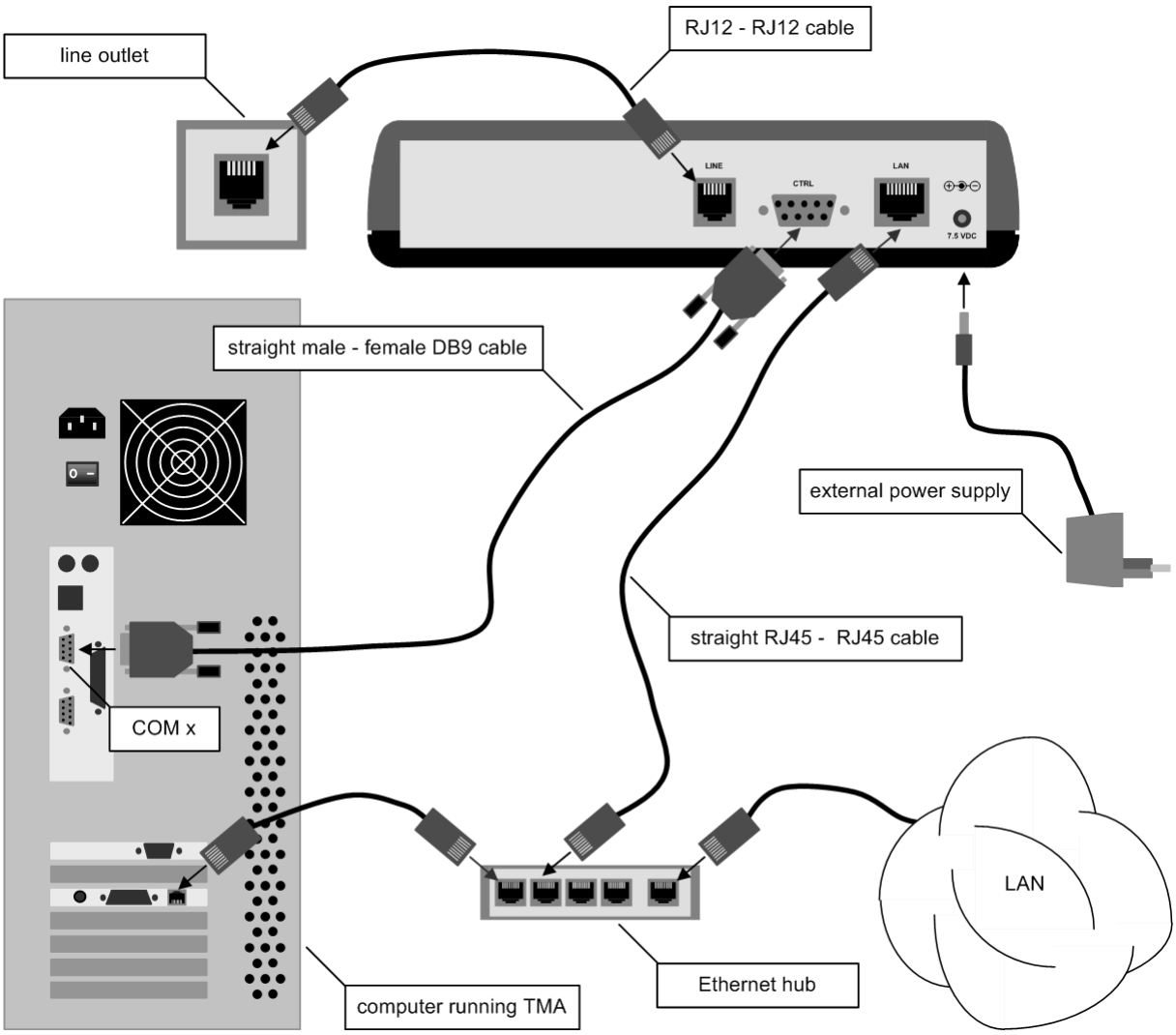
MU-2.6.2 Connexion des différentes parties du Routeur Telindus 1421 SHDSL

Le tableau qui suit donne un aperçu des pièces situées à l'arrière du Routeur Telindus 1421 SHDSL et indique leur fonction:

Etiquette	Fonction
7,5/9 V CC	Il s'agit de l'entrée d'alimentation. Insérez la fiche de l'alimentation externe dans cette prise. **Remarque importante** Dans le cas d'un … • Routeur Telindus 1421 SHDSL version 1 pair, la tension d'entrée est de 7,5 V CC. • Routeur Telindus 1421 SHDSL version 2 pair, la tension d'entrée est de 9 V CC. Reportez-vous à MR-8.13 - Power requirements page 394 pour les spécifications électriques du Routeur Telindus 1421 SHDSL.
LAN	Ce connecteur RJ45 assure la connexion avec le LAN. Connectez un côté du câble RJ45 à RJ45 (non inclus) au connecteur LAN du Routeur Telindus 1421 SHDSL et l'autre côté à une sortie réseau. Si vous souhaitez connecter le Routeur Telindus 1421 SHDSL à … • une sortie réseau Ethernet traditionnelle, utilisez un câble RJ45 croisé. • une plate-forme Ethernet, utilisez un câble RJ45 droit. Reportez-vous à MR-8.2 - LAN interface specifications page 387 pour les spécifications de ce connecteur.
CTRL	Ce connecteur femelle à 9 broches subD est le connecteur de commande. Vous pouvez raccorder ce connecteur à un port COM de votre PC à l'aide d'un câble DB9 mâle-femelle droit (non inclus). Cela vous permet de gérer le Routeur Telindus 1421 SHDSL localement, en utilisant TMA, CLI, ATWIN, etc. Vous pouvez également raccorder ce connecteur à un concentrateur, à des fins de gestion également. Reportez-vous à MR-8.3 - Control connector specifications page 388 pour les spécifications de ce connecteur.
LIGNE	Ce connecteur RJ12 assure la connexion avec la ligne SHDSL. Connectez un côté du câble RJ12 à RJ12 (non inclus) au connecteur LIGNE du Routeur Telindus 1421 SHDSL et l'autre côté à une sortie SHDSL. Pour des performances optimales, les paires de ligne utilisées doivent être des paires torsadées. Reportez-vous à MR-8.1 - SHDSL line specifications page 385 pour les spécifications de ce connecteur.

MU-2.6.3 Connexion du Routeur Telindus 1421 SHDSL - exemple

La figure qui suit montre une configuration Routeur Telindus 1421 SHDSL typique:



Dans cette configuration…

- Le connecteur LIGNE est raccordé à une sortie de ligne SHDSL à l'aide d'un câble RJ12 - RJ12. Le Routeur Telindus 1421 SHDSL est alors connecté au WAN. Vous pouvez, par exemple, connecter le Routeur Telindus 1421 SHDSL à un réseau distant par le biais d'une ligne louée. Reportez-vous à MU-1.2 - Routeur Telindus 1421 SHDSL applications page 6 pour certaines applications typiques.
- Le connecteur CTRL est raccordé au port COM d'un ordinateur par le biais d'un câble mâle-femelle DB9 droit. Vous pouvez ainsi, par exemple, commander le Routeur Telindus 1421 SHDSL localement en utilisant TMA (CLI), CLI, ATWIN, etc.
- Le connecteur LAN est raccordé à la plate-forme Ethernet en utilisant un câble RJ45 - RJ45 droit. Le Routeur Telindus 1421 SHDSL est alors connecté à votre réseau local (LAN).
- L'alimentation externe est connectée à l'entrée d'alimentation.

Pour des performances optimales, les paires de ligne utilisées doivent être des paires torsadées.

MU-2.7 Témoins à DEL du panneau avant

Cette section donne un aperçu des diodes du panneau avant et précise ce qu'elles indiquent. Le tableau suivant donne un aperçu de ce chapitre:

- MU-2.7.1 - Présentation des diodes du panneau avant page 22
- MU-2.7.2 - Diode de mise sous tension (PWR) page 23
- MU-2.7.3 - Diode de liaison de ligne LED (LINE LNK1 / LNK2) page 23
- MU-2.7.4 - Diode de données de ligne (LINE ACT) page 23
- MU-2.7.5 - Diode LAN (LAN ACT) page 24

MU-2.7.1 Présentation des diodes du panneau avant

Lorsque toutes les connexions sont assurées et que le Routeur Telindus 1421 SHDSL est sous tension, les diodes situées sur le panneau avant indiquent l'état en cours de l'unité.

La figure qui suit montre les témoins à diodes de la face avant du Routeur Telindus 1421 SHDSL:

Etat des diodes

Une diode du panneau avant peut refléter différents états selon la manière dont elle s'allume. Les diodes de la face avant peuvent s'allumer de la manière suivante:

Etat de la diode	Cycle d'activité de DEL	Description
Eteinte	0 %	La DEL ne s'allume jamais.
Allumée	100 %	La DEL reste en permanence allumée.
Clignotante	50 %	La DEL s'allume et s'éteint en alternance pendant le même nombre de secondes
Clignotante de manière irrégulière	20 %	La DEL ne s'allume que pendant 20 % du temps.
Essentiellement arrêtée	-	La diode s'allume occasionnellement, sans cycle d'allumage fixe.
Essentiellement en marche	-	La diode s'éteint occasionnellement, sans cycle fixe.
Surveillance	-	La DEL s'allume de manière irrégulière. Par exemple, elle s'allume à détection d'un certain signal, ce qui veut dire qu'elle surveille ce signal.

MU-2.7.2 Diode de mise sous tension (PWR)

La diode d'alimentation indique:

Etat DEL	Description
Eteinte	Aucune tension d'entrée.
Clignotante	Echec de l'autotest effectué durant la séquence d'initialisation. Dans cet état, les diodes ACT restent en permanence allumées.
Allumée	Le Routeur Telindus 1421 SHDSL est sous tension et la séquence d'initialisation a été réalisée avec succès. Si le Routeur Telindus 1421 SHDSL reste en mode d'initialisation, les diodes ACT restent allumées en permanence pour signaler cet état de fait. Reportez-vous à MR-7.1 - What is boot, loader and application software? page 375 pour de plus amples informations sur le mode d'initialisation.

MU-2.7.3 Diode de liaison de ligne LED (LINE LNK1 / LNK2)

Cette diode reflète l'état de la ligne:

Etat DEL	Description
Eteinte	Aucune réponse de l'établissement de la liaison. Rien n'est connecté à la ligne.
Clignotante	L'établissement de la ligne est en cours.
Allumée	L'établissement de la ligne a réussi. La couche 1 est active.

La diode LINE LNK2 existe uniquement sur un Routeur Telindus 1421 SHDSL version 2 pair.

MU-2.7.4 Diode de données de ligne (LINE ACT)

Cette diode reflète l'état des données utilisateur sur la ligne:

Etat DEL	Description
Eteinte	La couche 2 est inactive.
Surveillance	La couche 2 est active et les données utilisateur sont disponibles (données de transmission et de réception).
Allumée	La couche 2 est active, mais aucune donnée utilisateur n'est disponible.

MU-2.7.5 Diode LAN (LAN ACT)

Cette diode reflète l'état de la liaison et surveille les données utilisateur sur l'interface LAN:

Etat DEL	Description
Eteinte	Rien n'est connecté à l'interface LAN.
Surveillance	La liaison Ethernet est active et le LAN est actif.
Allumée en permanence	La liaison Ethernet est active, mais aucune activité sur le LAN.

MU-3 Commutateurs DIP du Routeur Telindus 1421 SHDSL

Ce chapitre localise les commutateurs DIP sur la carte mère du Routeur Telindus 1421 SHDSL. Il donne un aperçu de leur fonction et explique comment modifier leurs réglages.

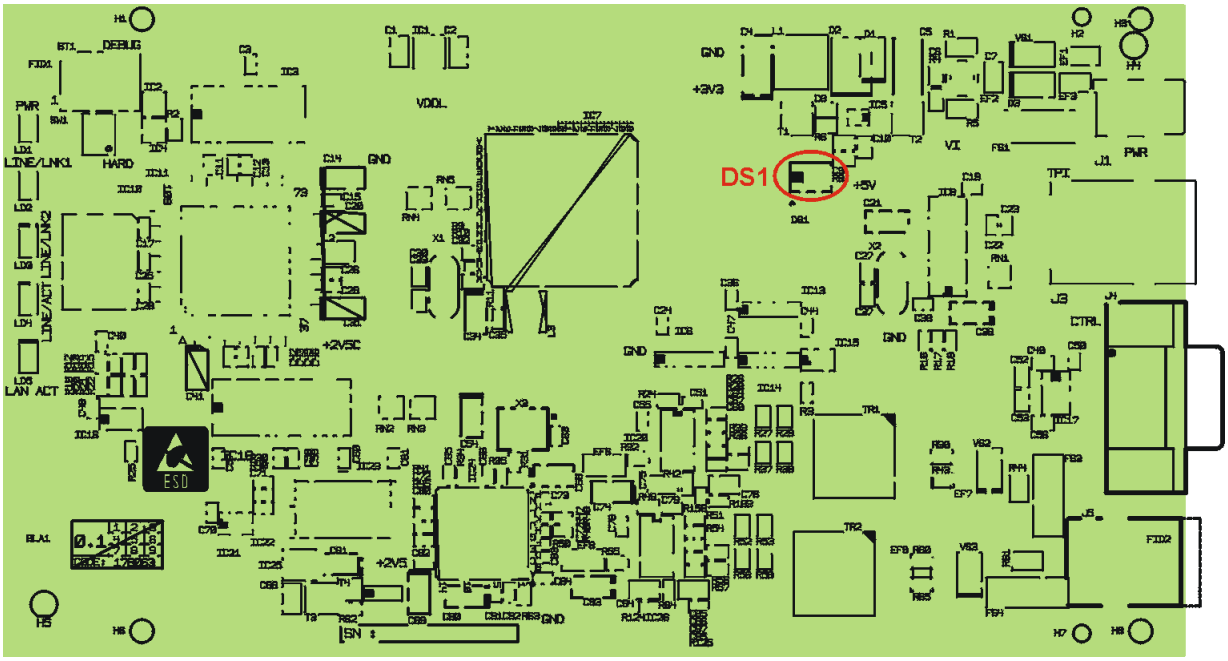
Le tableau suivant donne un aperçu de ce chapitre:

- MU-3.1 - La carte mère du Routeur Telindus 1421 SHDSL page 27
- MU-3.2 - Commutateurs DIP du Routeur Telindus 1421 SHDSL page 28
- MU-3.3 - Ouverture et fermeture du boîtier page 29

Les réglages par défaut sont imprimés en **gras**.

MU-3.1 La carte mère du Routeur Telindus 1421 SHDSL

La figure ci-dessous illustre la position des commutateurs DIP sur la carte mère du Routeur Telindus 1421 SHDSL:



MU-3.2 Commutateurs DIP du Routeur Telindus 1421 SHDSL

Le tableau qui suit donne un aperçu des commutateurs DIP sur la barrette de commutateurs DIP DS1:

Nom du commutateur DIP	DS1 no.	Réglage	Fonction
Mode de charge	1	**on**	Fonctionnement normal.
		off	Démarrage en mode de charge. Reportez-vous à MR-7.6 - Downloading application or loader software in loader mode page 381.
Chargement par défaut configuration	2	**on**	Fonctionnement normal.
		off	Charger la configuration par défaut. Reportez-vous à MU-5.5.4 - Chargement de la configuration par défaut en utilisant un commutateur DIP page 79.

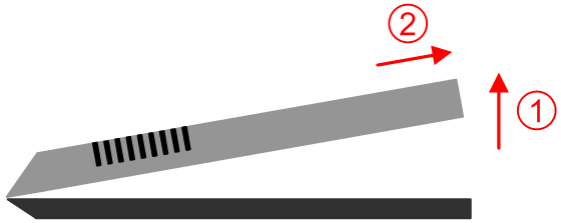
Reportez-vous à MU-3.3 - Ouverture et fermeture du boîtier page 29 pour voir comment ouvrir le boîtier pour modifier les réglages des commutateurs DIP.

MU-3.3 Ouverture et fermeture du boîtier

Si vous souhaitez modifier les réglages des commutateurs DIP du Routeur Telindus 1421 SHDSL, vous devez ouvrir et refermer le boîtier du Routeur Telindus 1421 SHDSL. Cette section explique comment faire.

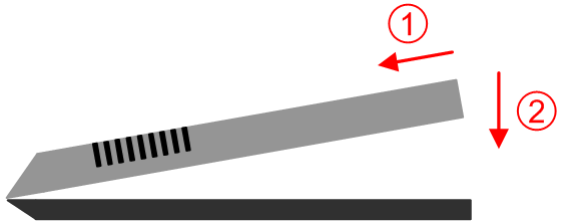
Ouverture du boîtier

Pour ouvrir le boîtier du Routeur Telindus 1421 SHDSL, procédez de la façon suivante:

Etape	Action
1	Débranchez l'alimentation externe.
2	Désserrez les deux vis situées à l'arrière du boîtier.
3	Déposez le capot de la façon suivante: 1. Soulevez délicatement l'arrière du capot sur quelques centimètres. 2. Retirez lentement le capot vers l'arrière en le sortant du nez du boîtier. 

Fermeture du boîtier

Pour fermer le boîtier du Routeur Telindus 1421 SHDSL, procédez de la façon suivante:

Etape	Action
1	Replacez le capot de la façon suivante: 1. Poussez lentement le capot sous le nez du boîtier. 2. Abaissez l'arrière du capot. 3. Tirez l'arrière du capot vers le bas, en encliquant le capot et le fond ensemble. 
2	Serrez les deux vis situées à l'arrière du boîtier.
3	Rebranchez l'alimentation externe.

MU-4 Maintenance du Routeur Telindus 1421 SHDSL

Après avoir installé le Routeur Telindus 1421 SHDSL, vous pouvez procéder à la configuration du Routeur Telindus 1421 SHDSL. Vous pouvez le faire en utilisant les outils de maintenance ou de gestion présentés au point MU-1.3 - Outils de gestion et de maintenance page 7.

Ce chapitre donne une description rapide de l'un de ces outils: L'application de maintenance Telindus (TMA). Il présente la TMA et décrit comment lancer une session du Routeur Telindus 1421 SHDSL. Il présente également la terminologie concernant la gestion d'une unité Telindus. De plus, il explique pourquoi et comment ajouter un objet à l'arborescence.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-4.1 - Maintenance du Routeur Telindus 1421 SHDSL avec TMA page 31
- MU-4.2 - Introduction à la terminologie de gestion page 37
- MU-4.3 - Les objets dans l'arborescence Routeur Telindus 1421 SHDSL page 41
- MU-4.4 - Ajout d'un objet dans l'arborescence page 43
- MU-4.5 - Routeur Telindus 1421 SHDSL aperçu des attributs page 48

MU-4.1 Maintenance du Routeur Telindus 1421 SHDSL avec TMA

Premièrement, cette section présente la TMA. Elle décrit ensuite comment lancer une session sur le Routeur Telindus 1421 SHDSL. Le tableau suivant donne un aperçu de ce chapitre:

- MU-4.1.1 - Qu'est-ce que la TMA? page 32
- MU-4.1.2 - Comment connecter la TMA? page 32
- MU-4.1.3 - Connexion avec la TMA par le connecteur de commande page 33
- MU-4.1.4 - Connexion TMA par un réseau IP page 35

MU-4.1.1 Qu'est-ce que la TMA?

TMA est l'acronyme de Telindus Maintenance Application. La TMA est un progiciel Windows gratuit qui vous permet d'assurer la maintenance du Routeur Telindus 1421 SHDSL, c'est-à-dire d'accéder à ses attributs de configuration et d'observer son état, ses performances et ses informations d'alarme à l'aide d'une interface utilisateur graphique très conviviale.

La TMA est un excellent outil de gestion intégrale des dispositifs d'accès Telindus. Lorsque vous utilisez la TMA en combinaison avec un système de gestion de réseau tel que HP OpenView, il vous est possible de gérer des réseaux complets à partir d'un site central.

Consultez le manuel TMA (PDF) pour voir comment installer la TMA et se familiariser avec l'interface utilisateur.

Vous aurez besoin d'une nouvelle version de distribution de fichiers modèles si des modifications ont été apportées aux attributs du Routeur Telindus 1421 SHDSL. Les fichiers les plus récents et le moteur TMA peuvent toujours être téléchargés à partir du site web Telindus à www.telindusproducts.com/TMA.

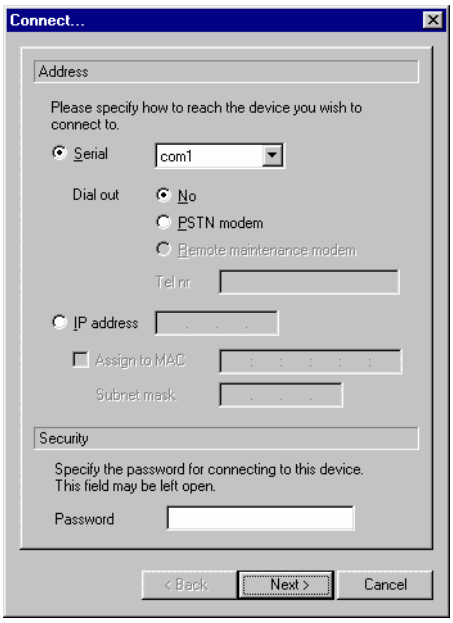
MU-4.1.2 Comment connecter la TMA?

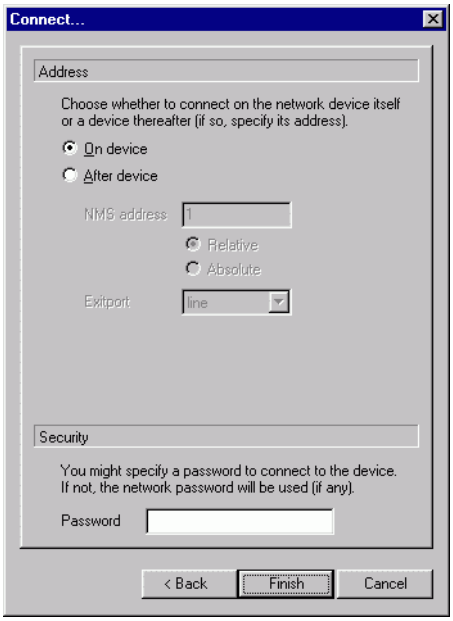
Il existe deux manières d'établir une connexion entre l'ordinateur utilisant la TMA et le Routeur Telindus 1421 SHDSL:

- par une connexion série, c'est-à-dire par le biais du connecteur de commande du Routeur Telindus 1421 SHDSL. Reportez-vous à MU-4.1.3 - Connexion avec la TMA par le connecteur de commande page 33.
- par une connexion IP, c'est-à-dire par le biais du connecteur LAN du Routeur Telindus 1421 SHDSL. Reportez-vous à MU-4.1.4 - Connexion TMA par un réseau IP page 35.

MU-4.1.3 Connexion avec la TMA par le connecteur de commande

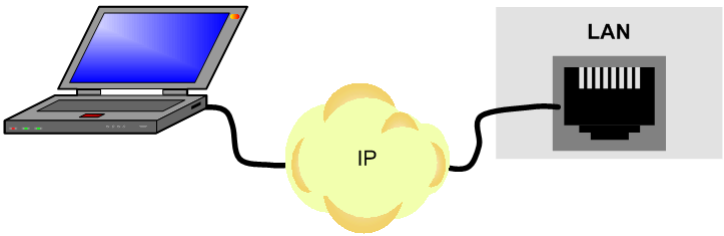
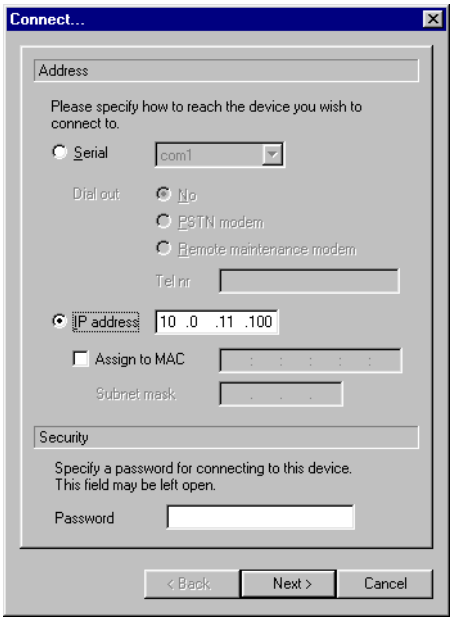
Pour établir une connexion entre la TMA et le Routeur Telindus 1421 SHDSL par le connecteur de commande, procédez de la façon suivante:

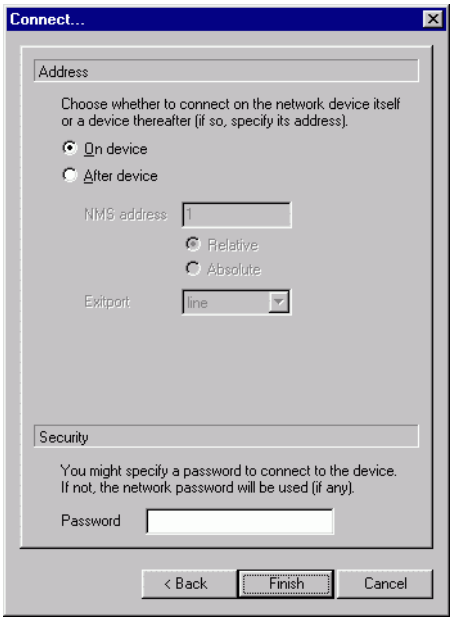
Etape	Action
1	Connectez un port série de votre ordinateur (p. ex. COM1) par un câble mâle-femelle droit DB9 au connecteur de commande du Routeur Telindus 1421 SHDSL.
2	Lancer la TMA.
3	Dans la fenêtre TMA, soit … • sélectionnez dans la barre de menu: *Connect* → *Device*… • ou pressez la touche de raccourci: Ctrl+N • ou cliquez sur le bouton *Connect to device*: La fenêtre *Connect*… (à une unité) apparaît comme dans la figure suivante: 
4	Dans la fenêtre *Connect*… (à une unité), spécifiez: • Sélectionnez l'option *Serial* et spécifiez le port COM de votre ordinateur auquel le Routeur Telindus 1421 SHDSL est connecté. • Si un mot de passe a été configuré au préalable dans le Routeur Telindus 1421 SHDSL renseignez aussi le champ du mot de passe.
5	cliquez sur le bouton *Next* >. ⇒La seconde fenêtre *Connect*… s'affiche.

Etape	Action
6	Dans la fenêtre *Connect…* (sélectionnez une unité), procédez de la façon suivante pour vous connecter au … • local Routeur Telindus 1421 SHDSL: sélectionnez *On device*. • distant Routeur Telindus 1421 SHDSL: - sélectionnez *After device*. - Entrez 1 dans le champ *NMS address*. - Sélectionnez *Relative*. - Si un mot de passe a préalablement été configuré dans l'unité distante Routeur Telindus 1421 SHDSL, renseignez également le champ du mot de passe.  Vous ne pouvez vous connecter à une unité distante Routeur Telindus 1421 SHDSL que si la liaison de données est active.
7	cliquez sur le bouton *Finish* .
8	Après quelques secondes, les attributs du Routeur Telindus 1421 SHDSL s'affichent dans la fenêtre TMA.

MU-4.1.4 Connexion TMA par un réseau IP

Pour établir une connexion entre la TMA et le Routeur Telindus 1421 SHDSL par un réseau IP, procédez de la façon suivante:

Etape	Action
1	Connectez le réseau IP … • au port réseau de votre PC, • au connecteur LAN du Routeur Telindus 1421 SHDSL. 
2	Lancer la TMA.
3	Dans la fenêtre TMA, soit … • sélectionnez dans la barre de menu: *Connect* → *Device…* • ou pressez la touche de raccourci: Ctrl+N • ou pressez le bouton *Connect to device*: La fenêtre *Connect…* (à une unité) s'affiche dans la figure suivante: 
4	Dans la fenêtre *Connect…* (à une unité), spécifiez: • Sélectionnez l'option *IP address* et entrez l'adresse IP du Routeur Telindus 1421 SHDSL. • Si un mot de passe a préalablement été configuré dans le Routeur Telindus 1421 SHDSL renseignez également le champ du mot de passe. Avant de pouvoir établir une connexion par un réseau IP, vous devez configurer une adresse IP et une passerelle par défaut dans le Routeur Telindus 1421 SHDSL. Pour ce faire, connectez d'abord la TMA au Routeur Telindus 1421 SHDSL par le biais du connecteur de commande, puis configurez une adresse IP et une passerelle par défaut. Reportez-vous à MU-5.2 - Configuration d'adresses IP page 52.
5	cliquez sur le bouton *Next* >. ⇒La seconde fenêtre *Connect…* s'affiche.

Etape	Action
6	Dans la fenêtre *Connect…* (sélectionnez une unité), procédez de la façon suivante pour vous connecter au … • local Routeur Telindus 1421 SHDSL: sélectionnez *On device*. • distant Routeur Telindus 1421 SHDSL: - sélectionnez *After device*. - Entrez 1 dans le champ *NMS address*. - Sélectionnez *Relative*. - Si un mot de passe a préalablement été configuré dans l'unité distante Routeur Telindus 1421 SHDSL, renseignez également le champ du mot de passe.  Vous ne pouvez vous connecter à une unité distante Routeur Telindus 1421 SHDSL que si la liaison de données est active.
7	cliquez sur le bouton *Finish* .
8	Après quelques secondes, les attributs du Routeur Telindus 1421 SHDSL s'affichent dans la fenêtre TMA.

MU-4.2 Introduction à la terminologie de gestion

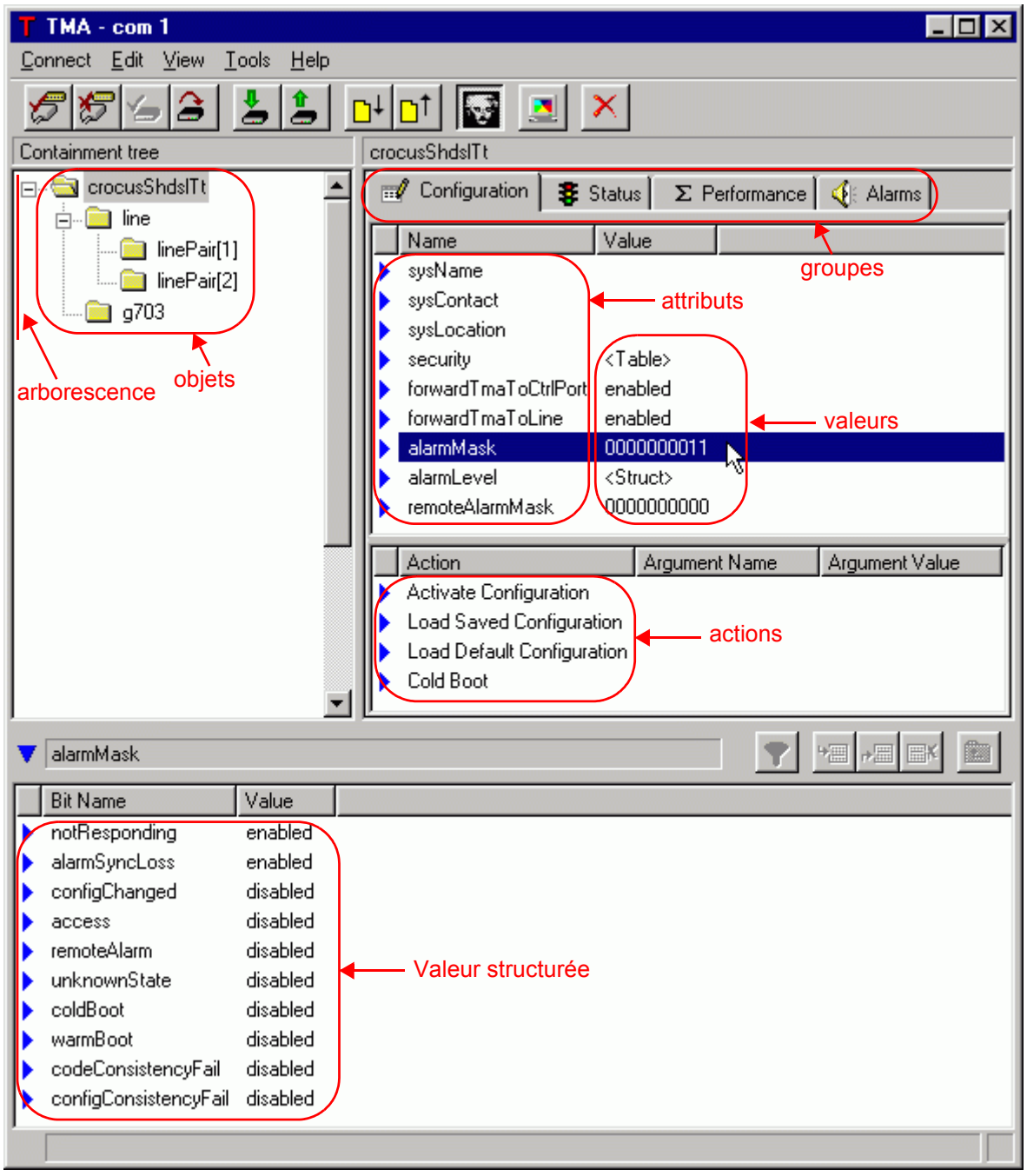
Cette section présente brièvement la terminologie concernant la gestion d'une unité Telindus. Elle définit également des termes tels qu'arborescence, groupe, objet, attribut, valeur et action.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-4.2.1 - Représentation graphique de l'arborescence page 38
- MU-4.2.2 - Terminologie d'arborescence page 39

MU-4.2.1 Représentation graphique de l'arborescence

La représentation graphique la plus complète de l'arborescence est fournie dans la TMA. La figure qui suit décrit la fenêtre TMA qui affiche une arborescence:



Reportez-vous à MU-4.2.2 - Terminologie d'arborescence page 39 pour une explication des termes associés à l'arborescence.

MU-4.2.2 Terminologie d'arborescence

Reportez-vous à MU-4.2.1 - Représentation graphique de l'arborescence page 38 pour voir une représentation d'une arborescence.

Le tableau qui suit explique la terminologie associée à l'arborescence:

Terme	Description
arborescence	L'arborescence représente la structure hiérarchique du Routeur Telindus 1421 SHDSL. Elle se compose d'un certain nombre d'objets qui sont classés à la manière d'un arbre. Cet arbre ressemble à une structure de répertoires Windows: • c'est également une structure par niveaux, dont les nœuds peuvent être agrandis ou réduits. • Les objets de l'arborescence peuvent être comparés aux répertoires de fichiers. • les objets contiennent des attributs, comme les répertoires de fichiers contiennent des fichiers.
objet	Un objet représente une interface physique, une application ou une combinaison des deux. Chaque objet dispose de son propre ensemble d'attributs.
objet parent et objet associé	Certains objets ne sont pas présents dans l'arborescence par défaut. Si vous souhaitez utiliser les fonctions associées à un tel objet, vous devez d'abord ajouter cet objet. Ajoutez toujours un objet sous un autre. L'objet que vous ajoutez est appelé objet associé. L'objet sous lequel vous ajoutez cet objet associé est appelé objet parent. Les objets que vous pouvez ajouter sont souvent signalés comme *objets utilisateur*.
nom d'indice	Parfois, plus d'un objet est présent dans l'arborescence. Les différents objets se distinguent les uns des autres par l'ajout d'un indice, p. ex. linePair[1] et linePair[2], où 1 et 2 sont les indices. Les objets associés se voient également affecter un indice (par l'utilisateur, lorsque celui-ci ajoute l'objet). Un nom d'indice est souvent désigné comme *indice*, *valeur d'instance* ou *nom d'instance*.
attribut	Un attribut est un paramètre relatif à un objet donné. Il a une certaine valeur.
valeur	Un attribut a une certaine valeur … • que l'on peut modifier dans le cas d'un attribut de configuration (à condition toutefois qu'il ne soit pas protégé en écriture) • que l'on peut exclusivement lire dans le cas d'un attribut d'état, de performance et d'alarme.

Terme	Description
valeur structurée	Certaines valeurs d'attribut contiennent des valeurs sous-jacentes: une valeur structurée. Ces valeurs apparaissent dans la fenêtre de valeur structurée. Si un attribut contient des valeurs structurées, une chaîne binaire, <Table> ou <Struct> s'affiche après l'attribut: • une chaîne binaire est une série de bits. La valeur de chacun de ces bits peut être 0 or 1, on ou off, activé ou désactivé. • une table contient des colonnes et des rangées. Chaque colonne contient un attribut (qui, à son tour, peut avoir une valeur structurée). Chaque rangée est une entrée dans la table. • une structure contient des colonnes, mais une seule rangée. Une structure peut être comparée à un attribut contenant plusieurs “sous-attributs”. Une valeur structurée est souvent désignée comme *chaîne binaire*, *table*, *structure* ou *valeur complexe*.
élément	Un élément est un attribut dans une valeur structurée. En d'autres termes, ils peuvent être considérés comme “sous-attributs”.
groupe	Les groupes contiennent un ensemble d'attributs reliés par leur fonctionnalité. Il existe quatre groupes dans la TMA, qui correspondent aux quatre onglets de la fenêtre d'attributs: • configuration, • état, • performance, • alarmes
action	Associé à un objet, un groupe peut se voir affecter telles ou telles actions. Ces actions s'affichent dans la fenêtre d'action.

MU-4.3 Les objets dans l'arborescence Routeur Telindus 1421 SHDSL

Le tableau qui suit répertorie les différents objets de l'arborescence du Routeur Telindus 1421 SHDSL. Il spécifie également les objets présents par défaut, que vous deviez les ajouter ou qu'ils soient ajoutés automatiquement.

> telindus1421Router
>> lanInterface
>> wanInterface
>>> atm
>>> frameRelay
>>> ppp
>>> hdlc
>>> ligne
>>>> linePair[ ][1]
>>> repeater[ ][2]
>>> end[2]
>> bundle
>>>> pppBundle[ ][3]
>> router
>>> tunnels
>>> defaultNat
>>> nat[ ][3]
>>> manualSA[ ][3]
>>> routingFilter[ ][3]

1. En cas de version Routeur Telindus 1421 SHDSL 2 paires, deux objets linePair[ ] sont présents.
2. Non présent par défaut. Apparaît uniquement lors du réglage de l'attribut eocHandling. Reportez-vous à MU-5.3.3 - Configuration gestion EOC page 67.

>>> priorityPolicy[ ][3]

>>> trafficPolicy[ ][3]

>>> ospf

>>>> area[3]

>> bridge

>>> bridgeGroup

>>> vpnBridgeGroup[ ][3]

>>> accessList[ ][3]

>> snmp

>> management

>>> loopBack

>> fileSystem

>> operatingSystem

3. Non présent par défaut, doit être ajouté. Le nom de l'indice est défini par l'utilisateur. Reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43.

MU-4.4 Ajout d'un objet dans l'arborescence

Cette section explique pourquoi et comment ajouter un objet à l'arborescence. Elle explique ensuite pourquoi et comment se reporter à cet objet.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-4.4.1 - Pourquoi ajouter un objet dans l'arborescence? page 44
- MU-4.4.2 - Comment ajouter un objet dans l'arborescence? page 45
- MU-4.4.3 - Référence à un objet ajouté page 47

MU-4.4.1 Pourquoi ajouter un objet dans l'arborescence?

Pourquoi pouvez-vous ajouter un objet dans l'arborescence?

Certains objets ne sont pas présents par défaut dans l'arborescence, mais vous pouvez les ajouter vous-même parce que …

- ainsi, l'arborescence reste claire et facilement examinable,
- il se peut que vous n'ayez pas besoin des fonctions associées à un tel objet,
- il se peut que vous ayez besoin de plusieurs de ces objets, afin de pouvoir ajouter autant d'objets que vous le souhaitez.

Quand devez-vous ajouter un objet dans l'arborescence?

Si vous souhaitez utiliser les fonctions associées à un tel objet, vous devez d'abord ajouter cet objet.

Quels objets ajouter dans l'arborescence?

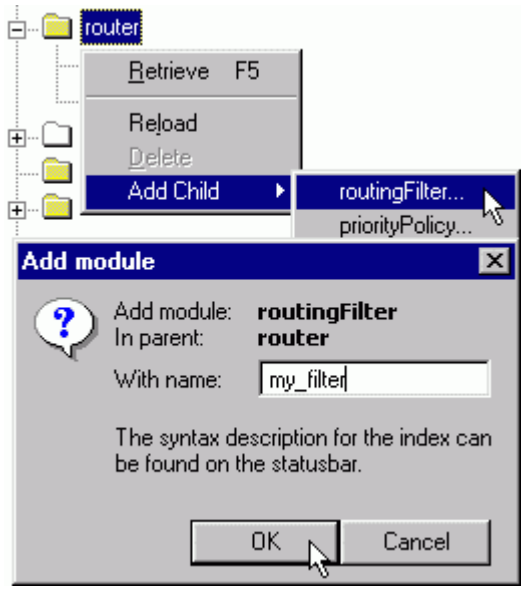
La section MU-4.3 - Les objets dans l'arborescence Routeur Telindus 1421 SHDSL page 41 vous donne un aperçu de tous les objets présents dans l'arborescence. Elle vous indique quels objets doivent être ajoutés avant de pouvoir les utiliser.

MU-4.4.2 Comment ajouter un objet dans l'arborescence?

Cette section vous montre, pour chaque outil de maintenance, comment ajouter un objet dans l'arborescence. La section qui suit, MU-4.4.3 - Référence à un objet ajouté page 47, vous montre comment vous “reporter” à cet objet ajouté ailleurs dans l'arborescence.

Ajout d'un objet dans la TMA

Etape	Action
1	Cliquez à droite sur l'objet parent (p. ex. router). ⇒Un menu déroulant apparaît.
2	Dans ce menu déroulant, sélectionnez *Add Child…* et sélectionnez l'objet associé que vous souhaitez ajouter (p. ex. routingFilter). ⇒Une fenêtre déroulante apparaît.
3	Dans la fenêtre déroulante, entrez le nom d'indice (c'est-à-dire la valeur d'instance) de l'objet associé (p. ex. my_filter) et cliquez *OK*. ⇒Le nouvel objet associé est créé (p. ex. routingFilter[my_filter]).



Ajout d'un objet dans (TMA) CLI

Etape	Action
1	Entrez l'objet parent (p. ex. `select router`).
2	Entrez la commande suivante: `réglez {sélectionnez childObjectName[instanceValue]{}}` où `instanceValue` est une chaîne de votre choix. (p. ex. `réglez {select routingFilter[my_filter]{}}`) ⇒Le nouvel objet associé est créé.

Ajout d'un objet dans ATWIN

Etape	Action
1	Entrez l'objet parent (p. ex. allez à l'objet router et pressez la touche entrée). ⇒La fenêtre ATWIN montre les sous-objets et les attributs de l'objet parent.
2	Allez à la ligne affichant la chaîne `<CREATE INSTANCE>` et sélectionnez le nom de l'objet que vous souhaitez ajouter (p. ex. `routingFilter <CREATE INSTANCE>`) puis pressez la touche entrée. ⇒Une nouvelle fenêtre apparaît, qui affiche la chaîne `Give the instanceValue`.
3	Pressez la touche entrée et entrez le nom d'indice (c'est-à-dire la valeur d'instance) de l'objet associé (p. ex. my_filter) puis pressez une nouvelle fois la touche entrée. ⇒Le nouvel objet associé est créé (p. ex. `>routingFilter[name:my_filter]`).

Ajout d'un objet dans l'interface web

Etape	Action
1	Entrez l'objet parent (p. ex. sélectionnez l'objet router et double-cliquez dessus ou cliquez *Open*). ⇒La fenêtre Web Interface montre les sous-objets et les attributs de l'objet parent.
2	Sélectionnez la ligne affichant la chaîne `<CREATE INSTANCE>` et le nom de l'objet que vous souhaitez ajouter (p. ex. `routingFilter <CREATE INSTANCE>`) et double-cliquez dessus ou cliquez *Open*. ⇒Une nouvelle fenêtre apparaît, qui affiche la chaîne `Give the instanceValue`.
3	Entrez le nom d'indice (c'est-à-dire la valeur d'instance) de l'objet associé (p. ex. my_filter) et cliquez *exit*. ⇒Le nouvel objet associé est créé (p. ex. `>routingFilter[name:my_filter]`).

MU-4.4.3 Référence à un objet ajouté

Qu'est-ce que la référence à un objet ajouté?

Si, à un endroit donné de l'arborescence, vous souhaitez appliquer la fonction associée à un objet que vous avez ajouté, vous devez vous référer à cet objet.

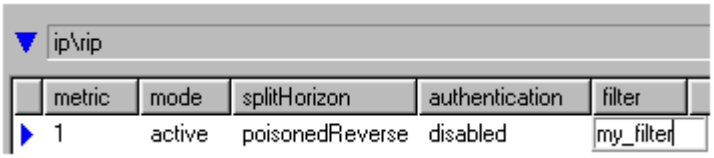
Comment se référer à un objet ajouté?

Certains attributs vous permettent d'entrer le nom d'indice (c'est-à-dire la valeur d'instance que vous avez affectée à l'objet) d'un objet ajouté. Ce faisant, la fonction associée à cet objet s'applique ici.

Exemple

Supposons que vous créiez un objet routingFilter portant le nom d'indice my_filter. L'arborescence a alors la configuration suivante:

Maintenant, vous souhaitez utiliser ce filtre sur l'interface LAN. Dans ce cas, dans la structure ip/rip de l'objet lanInterface, entrez le nom d'indice de l'objet routingFilter sous l'élément “filter”. Cela donne:



MU-4.5 Routeur Telindus 1421 SHDSL aperçu des attributs

La partie référence de ce manuel explique tous les attributs du Routeur Telindus 1421 SHDSL. Un chapitre décrit un groupe d'attributs:

- chapitre MR-1 - Configuration attributes page 6,
- chapitre MR-2 - Status attributes page 168,
- chapitre MR-3 - Performance attributes page 278,
- chapitre MR-4 - Alarm attributes page 334.

MU-5 Configuration de base

Ce chapitre vous indique comment configurer les éléments de base du Routeur Telindus 1421 SHDSL. Cela vous permet d'accéder au Routeur Telindus 1421 SHDSL par le biais d'une connexion IP avec, par exemple, TMA. Il explique également comment configurer les mots de passe sur le Routeur Telindus 1421 SHDSL. De plus, une section est consacrée aux mesures de configuration, qui décrit comment activer une configuration, comment charger la configuration par défaut, etc. Une autre section vous donne des références sur les explications relatives aux principales caractéristiques et fonctions du Routeur Telindus 1421 SHDSL. La dernière section explique brièvement les points à vérifier si vous deviez connaître des problèmes lors de l'installation, de la configuration ou du fonctionnement du Routeur Telindus 1421 SHDSL.

Les points suivants donnent un aperçu de ce chapitre:

- MU-5.1 - Qu'est-ce qu'une interface? page 51
- MU-5.2 - Configuration d'adresses IP page 52
- MU-5.3 - Configuration de la ligne SHDSL page 64
- MU-5.4 - Configuration des mots de passe page 74
- MU-5.5 - Exécution des actions de configuration page 76
- MU-5.6 - Configuration des principales fonctions du Routeur Telindus 1421 SHDSL page 80
- MU-5.7 - Dépistage des erreurs Routeur Telindus 1421 SHDSL page 81

Reportez-vous au Manuel de référence pour un aperçu complet des attributs du Routeur Telindus 1421 SHDSL.

MU-5.1 Qu'est-ce qu'une interface?

Le terme interface, tel qu'il est utilisé dans ce manuel, peut se diviser en deux groupes:

Type d'interface	Description
physique	Une interface physique est une interface à laquelle il est physiquement possible de raccorder un câble. Une interface physique présente donc un connecteur physique. Elle dispose également de certains attributs de configuration qui contrôlent son fonctionnement. Par exemple: • L'interface de contrôle (CTRL). Elle est équipée d'un connecteur femelle subD à neuf broches auquel vous pouvez raccorder un connecteur mâle subD à neuf broches à des fins de maintenance. Elle dispose d'attributs de configuration tels que ctrlPortProtocol, cms2Address, etc. • L'interface LAN (LAN). Elle est équipée d'un connecteur femelle RJ45 auquel vous pouvez raccorder un connecteur mâle RJ45 pour la connexion à un réseau Ethernet. Elle dispose d'attributs de configuration tels que ip, vlan, etc. Parmi les autres exemples, citons l'interface d'horloge, les interfaces d'alarme, les interfaces de ligne xDSL, etc.
logique	Une interface logique est une interface à laquelle il est impossible de raccorder physiquement un câble. Une interface logique ne dispose donc d'aucun connecteur physique. Toutefois, elle fait partie de l'interface physique, mais à un niveau plus élevé. Une interface physique peut “contenir” plusieurs interfaces logiques. Elle dispose également de certains attributs de configuration qui contrôlent le fonctionnement de ces interfaces. Par exemple: • Un ATM PVC sur une ligne xDSL. La ligne xDSL est l'interface physique (elle dispose d'un connecteur physique), alors que l'ATM PVC est l'interface logique (elle est située à un niveau supérieur, c'est-à-dire au niveau du protocole de la couche 2). Il est possible d'avoir plusieurs ATM PVC sur une seule ligne xDSL. • Un VLAN sur l'interface LAN L'interface LAN est l'interface physique, le VLAN l'interface logique. Parmi les autres exemples, citons les tunnels L2TP, les liaisons d'un faisceau multiliaisons, les groupes de pontage, etc.

MU-5.2 Configuration d'adresses IP

La première chose que vous devez configurer sont les adresses IP du Routeur Telindus 1421 SHDSL. Cette section indique d'abord les mécanismes existants pour obtenir automatiquement une adresse IP. Elle montre ensuite où trouver les paramètres relatifs à l'IP. Enfin, cette section explique ces paramètres relatifs à l'IP.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-5.2.1 - Obtention automatique d'une adresse IP page 53
- MU-5.2.2 - Où trouver les paramètres IP? page 54
- MU-5.2.3 - Explication de la structure ip page 55

MU-5.2.1 Obtention automatique d'une adresse IP

Obtention d'une adresse IP sur l'interface LAN

Le Routeur Telindus 1421 SHDSL supporte le protocole BootP pour obtenir automatiquement une adresse IP sur son interface LAN.

Reportez-vous à MR-6 - Auto installing the Telindus 1421 SHDSL Router page 354 pour de plus amples informations sur l'auto-installation.

Obtention d'une adresse IP sur l'interface WAN

Dans le cas de …

- ATM, reportez-vous à MU-6.2.3 - Obtention automatique d'adresses IP dans ATM page 93.
- Frame Relay, reportez-vous à MU-6.3.3 - Obtention automatique d'adresses IP dans Frame Relay page 113.
- PPP(oA), reportez-vous à MU-6.4.2 - Obtention automatique d'adresses IP dans PPP page 126.

Une adresse IP obtenue à l'aide d'une procédure dynamique n'apparaît pas dans la fenêtre de configuration, mais peut être consultée dans la fenêtre d'état.

MU-5.2.2 Où trouver les paramètres IP?

Le tableau qui suit vous montre où trouver les paramètres IP des différentes interfaces IP:

Interface	Emplacement des paramètres IP
Interface LAN	Dans la ip structure de l'objet lanInterface: telindus1421Router/lanInterface/ip. **Remarque importante** Si vous réglez l'attribut de configuration telindus1421Router/lanInterface/mode sur bridging, alors le réglage de l'attribut de configuration telindus1421Router/lanInterface/ip est ignoré. Dans ce cas, si vous souhaitez gérer le Routeur Telindus 1421 SHDSL via IP, vous devez configurer une adresse IP dans l'objet bridgeGroup. telindus1421Router/bridge/bridgeGroup/ip.
VLAN sur l'interface LAN	Dans la ip structure de la table vlan située dans l'objet lanInterface: telindus1421Router/lanInterface/vlan/ip.
ATM PVC	Dans la structure ip de la pvcTable située dans l'objet atm: telindus1421Router/wanInterface/atm/pvcTable/ip.
Liaison PPP	Dans la structure ip de l'objet ppp: telindus1421Router/wanInterface/ppp/ip.
PVC relais trame	Vous trouvez la structure ip à deux niveaux: • dans l'objet frameRelay: telindus1421Router/wanInterface/frameRelay/ip. • dans l'attribut dlciTable: telindus1421Router/wanInterface/frameRelay/dlciTable/ip. La section MU-6.3.4 - Configuration d'adresses IP dans Frame Relay page 114 explique les raisons pour lesquelles vous pouvez configurer les paramètres IP à deux niveaux différents.
Tunnel L2TP	Dans la structure ip de la table l2tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/l2tpTunnels/ip.
Tunnel IPSEC L2TP	Dans la structure ip de la table ipsecL2tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/ipsecL2tpTunnels/ip.
Groupe de pontage	Dans la structure ip de l'objet bridgeGroup: telindus1421Router/bridge/bridgeGroup/ip.
Boucle arrière de gestion	Dans l'attribut ipAddress de l'objet loopback: telindus1421Router/management/loopback/ipAddress.

Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour une explication détaillée de la structure ip.

MU-5.2.3 Explication de la structure ip

La structure ip survenant dans plusieurs objets, elle ne sera décrite ici qu'une seule fois et mentionnée lorsque cela sera nécessaire. Reportez-vous à MU-5.2.2 - Où trouver les paramètres IP? page 54 pour l'emplacement de la structure ip.

Cette section répertorie tous les éléments qui peuvent être présents dans la structure ip. Toutefois, en fonction de l'interface, il est possible que tous ces éléments ne soient pas présents.

La structure ip contient les éléments suivants:

Elément	Description
address	Utilisez cet élément pour assigner une adresse IP à l'interface. L'adresse doit appartenir au réseau secondaire auquel l'interface est connectée. Par défaut:0.0.0.0 Gamme:max. 255.255.255.255 Si vous ne configurez pas explicitement une adresse IP locale en utilisant l'élément address, elle peut être apprise. Reportez-vous à MU-5.2.1 - Obtention automatique d'une adresse IP page 53. Une adresse IP obtenue à l'aide d'une procédure dynamique n'apparaît pas dans la fenêtre de configuration, mais peut être consultée dans la fenêtre d'état.
netMask	Utilisez cet élément pour assigner un masque de réseau secondaire IP à l'interface. Le masque de réseau secondaire définit le nombre d'unités IP pouvant être présentes sur le segment IP correspondant. Par défaut:255.255.255.0 Gamme:max. 255.255.255.255
secondaryIp	Utilisez cet élément pour créer des réseaux virtuels supplémentaires sur la même interface Ethernet. Par défaut:<néant> Gamme:table, voir ci-dessous La table secondaryIp contient les éléments address et netMask. Reportez-vous ci-dessus pour une explication plus détaillée de ces éléments.
remote	Utilisez cet élément pour affecter une adresse IP à l'extrémité distante d'un ATM PVC, une liaison PPP, un Frame Relay DLCI ou un tunnel L2TP. Par défaut:0.0.0.0 Gamme:max. 255.255.255.255 Si vous ne configurez pas explicitement une adresse IP locale en utilisant l'élément remote, elle peut être apprise. Reportez-vous à MU-5.2.1 - Obtention automatique d'une adresse IP page 53. Une adresse IP obtenue à l'aide d'une procédure dynamique n'apparaît pas dans la fenêtre de configuration, mais peut être consultée dans la fenêtre d'état.

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>acceptLocAddr</td><td>
Cet élément n'est présent que dans un profil de transmission d'acheminement ISDN (p. ex. defaultRouting).
Par défaut:activé
Gamme:activé / désactivé

En cas de liaison PPP(oA), il est possible d'apprendre l'adresse IP locale auprès de l'extrémité distante. Utilisez l'élément acceptLocAddr pour déterminer s'il convient d'accepter ou de rejeter l'adresse IP apprise:
<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>enabled</td><td>Si l'extrémité distante peut transmettre une adresse IP, l'adresse IP locale est apprise de l'extrémité distante. Même si vous configurez explicitement une adresse IP locale (p. ex. en utilisant l'élément addrPool ou unnumbered). En d'autres termes, si l'élément acceptLocAddr est réglé sur activé, l'adresse IP locale qui a été configurée est subordonnée à celle qui a été apprise.</td></tr>
<tr><td>disabled</td><td>L'adresse IP locale ne peut être apprise depuis l'extrémité distante.</td></tr>
</table>

Reportez-vous également à MU-6.4.2 - Obtention automatique d'adresses IP dans PPP page 126.

Une adresse IP obtenue à l'aide d'une procédure dynamique n'apparaît pas dans la fenêtre de configuration, mais peut être consultée dans la fenêtre d'état.
</td></tr>
</table>

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>acceptRemAddr</td><td>Cet élément n'est présent que dans un profil de transmission d'acheminement ISDN (p. ex. defaultRouting).
Par défaut:activé
Gamme:activé / désactivé

En cas de liaison PPP(oA), il est possible d'apprendre l'adresse IP distante auprès de l'extrémité distante. Utilisez l'élément acceptRemAddr pour déterminer s'il convient d'accepter ou de rejeter l'adresse IP apprise:

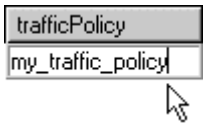
<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>enabled</td><td>Si l'extrémité distante peut transmettre une adresse IP, l'adresse IP distante est apprise de l'extrémité distante. Même si vous configurez explicitement une adresse IP locale (p. ex. en utilisant l'élément addrPool). En d'autres termes, si l'élément acceptRemAddr est réglé sur activé, l'adresse IP distante qui a été configurée est subordonnée à celle qui a été apprise.</td></tr>
<tr><td>disabled</td><td>L'adresse IP distante ne peut être apprise depuis l'extrémité distante.</td></tr>
</table>

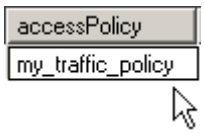
Reportez-vous également à MU-6.4.2 - Obtention automatique d'adresses IP dans PPP page 126.

Une adresse IP obtenue à l'aide d'une procédure dynamique n'apparaît pas dans la fenêtre de configuration, mais peut être consultée dans la fenêtre d'état.</td></tr>
<tr><td>unnumbered</td><td>Si vous ne configurez pas explicitement une adresse IP locale pour une liaison PPP(oA) en utilisant l'élément address , vous pouvez utiliser l'élément unnumbered pour "emprunter" l'adresse IP d'une autre interface pour laquelle une adresse IP est déjà configurée, conservant ainsi l'espace réseau et d'adressage.
Par défaut:<néant>
Gamme:0 ... 24 caractères

Pour ce faire, entrez le nom de l'interface comme valeur de l'élément unnumbered.
unnumbered
lan</td></tr>
<tr><td>gatewayPreference</td><td>Si vous ne configurez pas explicitement une adresse IP locale ou distante pour une liaison PPP(oA) en utilisant l'élément address et remote , ces adresses peuvent être apprises de l'extrémité distante. De plus, cet acheminement est automatiquement installé comme acheminement par défaut vers l'extrémité distante. Dans ce cas, vous pouvez utiliser l'élément gatewayPreference pour déterminer la préférence de cet acheminement par défaut. Reportez-vous à l'élément preference page 82 pour de plus amples informations.
Par défaut:80
Gamme:0 ... 90

Notez que si vous réglez l'élément gatewayPreference sur 0, l'acheminement n'est alors pas installé.</td></tr>
</table>

Elément	Description
mtu	Utilisez cet élément pour définir l'unité de transmission maximale (MTU) de l'interface. Par défaut:1500 Gamme:500 … 1650 **Qu'est-ce que le MTU?** L'unité de transmission maximale (MTU - Maximum Transmission Unit) est le paquet ou la trame de taille maximale, spécifiée en octets (huit bits), pouvant être envoyé sur un réseau par paquets ou par trames (p. ex. l'internet). Dans le cas de l'internet, il s'agit du protocole de contrôle de transmission (TCP) qui utilise la MTU pour déterminer la taille maximale de chaque paquet lors d'une transmission. Une MTU trop grande peut entraîner la retransmission si le paquet rencontre un routeur qui ne peut supporter un paquet de cette taille. Une MTU trop petite entraîne une en-tête relativement plus grande et des accusés de réception plus nombreux à envoyer et à traiter. La norme Ethernet MTU est 1500. La norme internet de facto MTU est 576, mais les but ISP suggèrent souvent d'utiliser 1500. Pour des protocoles autres que TCP, différentes tailles de MTU peuvent s'appliquer.
rip	Utilisez cet élément pour configurer les paramètres de l'IP du VLAN. Par défaut:- Gamme:structure, voir ci- Reportez-vous à MU-7.5.3 - Explication de la structure rip page 171 pour une explication détaillée de la structure rip.
trafficPolicy	Utilisez cet élément pour appliquer une politique de trafic aux données acheminées sur cette interface. Par défaut:<néant> Gamme:0 … 24 caractères Pour ce faire, entrez le nom d'indice de la politique de trafic que vous souhaitez utiliser. Vous pouvez créer la politique de trafic elle-même en ajoutant un objet trafficPolicy sous l'objet router et en configurant les attributs dans cet objet. **Exemple:** Si vous avez créé un objet trafficPolicy portant le nom d'indice my_traffic_policy (c'est-à-dire trafficPolicy[my_traffic_policy]) et que vous souhaitez appliquer cette politique de trafic ici, entrez le nom d'indice comme valeur de l'élément trafficPolicy.  Reportez-vous au… • MU-7.8 - Configuration de la politique de trafic et de priorité sur le routeur page 204 pour de plus amples informations sur les politiques. • MU-9.2 - Configuration des restrictions d'accès page 258 pour de plus amples informations sur les listes d'accès sortantes.

Elément	Description
accessPolicy	Utilisez cet élément pour appliquer une politique d'accès aux données acheminées sur cette interface. Par défaut:<néant> Gamme:0 … 24 caractères Alors qu'en utilisant l'élément trafficPolicy vous pouvez appliquer une liste d'accès *outbound* à l'interface, vous pouvez appliquer une liste d'accès *inbound* sur l'interface en utilisant l'élément accessPolicy. Pour ce faire, entrez le nom d'indice de la politique de trafic que vous souhaitez utiliser. Vous pouvez créer la politique de trafic elle-même en ajoutant un objet trafficPolicy sous l'objet router et en configurant les attributs dans cet objet. **Exemple:** Si vous avez créé un objet trafficPolicy portant le nom d'indice my_traffic_policy (c'est-à-dire trafficPolicy[my_traffic_policy]) et que vous souhaitez appliquer cette politique de trafic ici, entrez le nom d'indice comme valeur de l'élément trafficPolicy.  Reportez-vous à MU-9.2 - Configuration des restrictions d'accès page 258 pour de plus amples informations.
mgmtAccess	Utilisez cet élément pour activer ou désactiver l'accès de gestion par le biais de cette interface. Par défaut:activé Gamme:activé / désactivé Si vous réglez l'attribut mgmtAccess sur désactivé, vous ne pouvez pas accéder à la pile de protocoles par cette interface.
directedBroadcasts	Utilisez cet élément pour activer (transmettre) ou désactiver (refuser) les diffusions dirigées. Par défaut:activé Gamme:activé / désactivé **Qu'est-ce qu'une diffusion dirigée?** Une diffusion dirigée est un paquet IP destiné à un réseau (secondaire) complet. Par exemple, un paquet destiné à toutes les unités sur le réseau secondaire 192.168.48.0 avec le masque 255.255.255.0 a l'adresse de destination 192.168.48.255. C'est-à-dire tous dans la zone de réseau secondaire de l'adresse IP.
icmpRedirects	Utilisez cet élément pour activer ou désactiver la transmission des messages ICMP. Par défaut:activé Gamme:activé / désactivé **Qu'est-ce qu'une redirection ICMP?** Si icmpRedirects est activé et si le Routeur Telindus 1421 SHDSL reçoit un paquet IP sur l'interface pour laquelle … • la passerelle suivante se trouve sur la même interface, • l'adresse suivante se trouve sur le même réseau secondaire que la source, … alors il envoie un message ICMP à l'origine du paquet pour l'informer qu'un meilleur acheminement (plus court) existe.

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>igmp</td><td>Utilisez cet élément pour configurer le protocole multidiffusion IGMP.
Par défaut:désactivé
Gamme:énumérée, voir ci-

L'élément igmp a les valeurs suivantes:

<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>disabled</td><td>Les multidiffusions ne sont pas transmises sur cette interface.</td></tr>
<tr><td>proxy</td><td>Il s'agit d'une interface amont. Elle sert toujours de client pour le routeur amont.

Les multidiffusions sont toujours transmises sur cette interface.</td></tr>
<tr><td>router</td><td>Il s'agit d'une interface aval. Elle sert de demandeur ou de non demandeur IGMP en fonction de l'adresse IP.

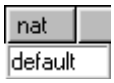
Les multidiffusions sont transmises sur cette interface si elles sont présentes dans la liste de membres multifdiffusion de l'interface amont.</td></tr>
</table>

Reportez-vous à What is IGMP? et IGMP topology page 235 pour de plus amples informations sur IGMP.</td></tr>
<tr><td>helpers</td><td>Utilisez cet élément pour activer la transmission de diffusions.
Par défaut:<néant>
Gamme:table, voir ci-dessous

Les diffusions IP limitées (addresse 255.255.255.255) et les diffusions de réseau (secondaire) pour un réseau directement connecté ne sont normalement pas transmises par le Routeur Telindus 1421 SHDSL. Toutefois, les applications client / serveur utilisent souvent ces diffusions lors de la mise en route pour découvrir le serveur sur le réseau. Si le serveur est un LAN distant, la détection peut échouer.

Par conséquent, si vous configurez une adresse IP de secours, l'adresse de diffusion reçue est remplacée par cette adresse IP de secours et les paquets sont ré-acheminés en utilisant l'adresse de destination. Les adresses IP de secours peuvent être configurées.

Le Routeur Telindus 1421 SHDSL remplace uniquement les adresses pour les protocoles qui sont sélectionnés dans l'attribut helperProtocols. Reportez-vous à telindus1421Router/router/helperProtocols page 88.</td></tr>
</table>

Elément	Description
nat	Utilisez cet élément pour activer la translation d'adresse de réseau sur l'interface. Par défaut:<néant> Gamme:0 … 24 caractères Pour ce faire, entrez le nom de l'objet NAT que vous souhaitez appliquer. • Si vous souhaitez appliquer les réglages NAT tels que définis dans l'objet router/defaultNat, entrez la chaîne “default“ comme valeur de l'élément nat.  • Si vous souhaitez appliquer les réglages NAT tels que définis dans un objet NAT que vous avez vous-mêmes ajouté (p. ex. router/nat[myNat]), entrez alors le nom d'indice de l'objet NAT (dans ce cas “myNat”) comme valeur de l'élément nat. Reportez-vous au… • MU-7.7 - Configuration de translation d'adresses page 185 pour de plus amples informations sur le NAT. • MR-1.9.2 - NAT configuration attributes page 98 pour une description complète des attributs de configuration NAT.

MU-5.2.4 Configuration d'une adresse IP sur l'interface LAN

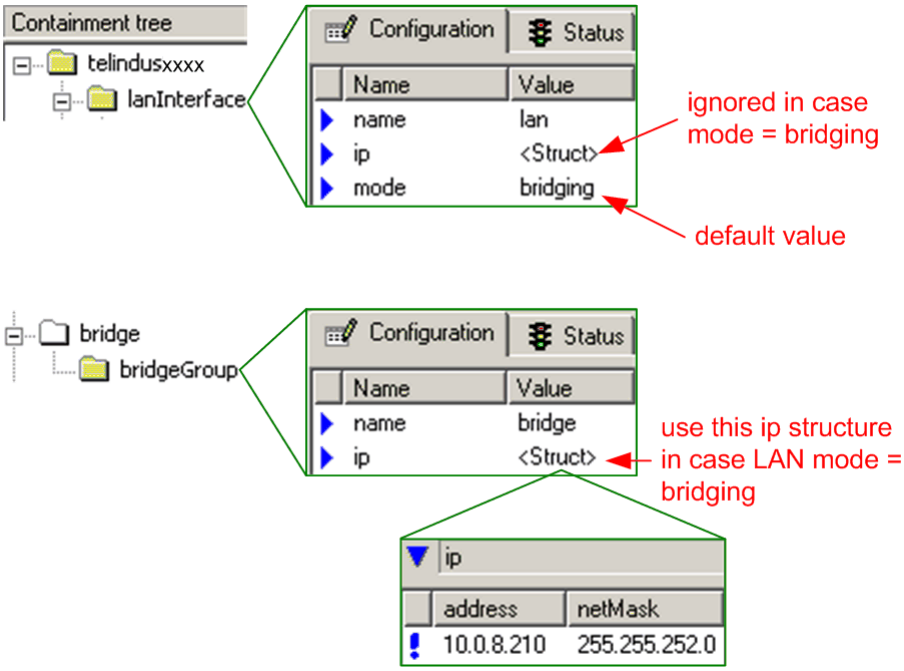
Lors de la configuration d'une adresse IP sur l'interface LAN, il existe deux scénarios différents:

- Le mode d'interface LAN est *bridging* (l'attribut de configuration telindus1421Router/lanInterface/mode est réglé sur bridging). Il s'agit du réglage par défaut.
- Le mode d'interface LAN est *routing* (l'attribut de configuration telindus1421Router/lanInterface/mode est réglé sur routing).

Mode d'interface LAN = pontage

Dans ce cas, les réglages de l'attribut de configuration telindus1421Router/lanInterface/ip sont ignorés. Si vous souhaitez gérer le Routeur Telindus 1421 SHDSL via IP, vous devez configurer une adresse IP dans l'objet bridgeGroup: telindus1421Router/bridge/bridgeGroup/ip.

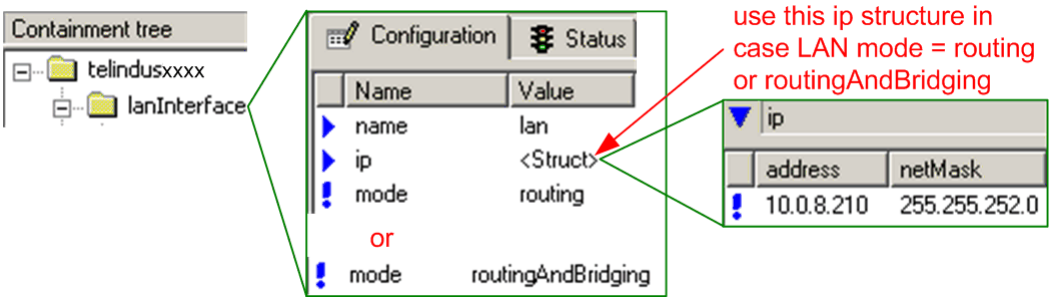
Supposons que vous souhaitiez affecter l'adresse IP 10.0.8.210 avec le masque de réseau secondaire 255.255.252.0 à l'interface LAN ; il convient alors de configurer les attributs correspondants de la façon suivante:



Mode d'interface LAN = acheminement

Dans ce cas, les réglages de l'attribut de configuration telindus1421Router/lanInterface/ip sont utilisés.

Supposons que vous souhaitiez affecter l'adresse IP 10.0.8.210 avec le masque de réseau secondaire 255.255.252.0 à l'interface LAN ; il convient alors de configurer les attributs correspondants de la façon suivante:



MU-5.3 Configuration de la ligne SHDSL

Lorsque vous souhaitez établir une connexion de ligne avec succès, vous devez configurer certains attributs de ligne. Cette section vous indique quels attributs de lignes sont essentiels. Elle vous donne également des informations complémentaires sur la manière de sélectionner une vitesse de ligne (gamme). Enfin, elle explique le concept d'alimentation de secours. Elle explique aussi comment configurer le Embedded Operations Channel (EOC).

Le tableau suivant donne un aperçu de ce chapitre:

- MU-5.3.1 - Principaux attributs de configuration de ligne SHDSL page 65
- MU-5.3.2 - Sélection d'une vitesse de ligne SHDSL (gamme) page 66
- MU-5.3.3 - Configuration gestion EOC page 67
- MU-5.3.4 - Information EOC récupérée page 69
- MU-5.3.5 - Sécurité d'alimentation page 73
- MU-5.3.6 - Utilisation d'un répéteur sur la ligne SHDSL page 73
- MU-5.3.7 - Compatibilité avec d'autres unités SHDSL page 73

MU-5.3.1 Principaux attributs de configuration de ligne SHDSL

Pour établlir avec succès une connexion de ligne, il est essentiel de régler correctement les attributs de configuration suivants:

Attribut	Objet de l'attribut
telindus1421Router/wanInterface/line/channel page 63	Pour la synchronisation, une unité doit être définie comme *centrale* et sa contrepartie distante comme *distante*. L'attribut channel influence également la synchronisation du Routeur Telindus 1421 SHDSL.
telindus1421Router/wanInterface/line/region page 63	Pour un fonctionnement correct, sélectionnez la norme SHDSL correcte. Normalement, le réglage auto doit suffire.
telindus1421Router/wanInterface/line/timingMode page 64	Pour une parfaite compatibilité avec les autres unités SHDSL, sélectionnez le mode de synchronisation adéquat. L'attribut timingMode influence également la synchronisation du Routeur Telindus 1421 SHDSL.
En cas de Routeur Telindus 1421 SHDSL version 1 paire, utilisez: • telindus1421Router/wanInterface/line/minSpeed page 67 • telindus1421Router/wanInterface/line/maxSpeed page 67 En cas de Routeur Telindus 1421 SHDSL version 2 paires, utilisez: • telindus1421Router/wanInterface/line/minSpeed2P page 68 • telindus1421Router/wanInterface/line/maxSpeed2P page 68	Pour une connexion de ligne réussie et de qualité, sélectionnez une vitesse appropriée (gamme). Reportez-vous à MU-5.3.2 - Sélection d'une vitesse de ligne SHDSL (gamme) page 66 pour de plus amples informations sur la vitesse (gamme).

Reportez-vous à MR-1.6 - SHDSL line configuration attributes page 62 pour un aperçu complet des attributs de configuration de ligne.

MU-5.3.2 Sélection d'une vitesse de ligne SHDSL (gamme)

Sélection d'une gamme de vitesse

Le Routeur Telindus 1421 SHDSL présente une fonction de vitesse autoconforme à la norme ITU-T G.994.1. Lors de la négociation, le Routeur Telindus 1421 SHDSL sélectionne une vitesse comprise entre la vitesse minimale et la vitesse maximale telles que définies par les attributs minSpeed(2P) et maxSpeed(2P).

Remarque importante

Dans le cas du Routeur Telindus 1421 SHDSL version 2 paires, définissez une gamme de vitesse *soit* sur la centrale *soit* sur la distante Routeur Telindus 1421 SHDSL, *mais pas sur les deux*. Sinon, les 2 paires de lignes pourraient fonctionner à une vitesse différente, ce qui est interdit.

Sélection d'une vitesse fixe

Si vous réglez les attributs minSpeed(2P) et maxSpeed(2P) sur la même valeur, le Routeur Telindus 1421 SHDSL fonctionne alors à une vitesse fixe.

Vitesse de ralentissement

Lorsque vous définissez une gamme de vitesses, le Routeur Telindus 1421 SHDSL tente toujours de fonctionner à la vitesse maximale. Si le modem à distance n'autorise pas cette vitesse ou si la qualité du signal se détériore, le Routeur Telindus 1421 SHDSL tente de sélectionner la vitesse immédiatement inférieure. En cas de nouvel échec, le Routeur Telindus 1421 SHDSL ralentit une nouvelle fois sa vitesse. Il procède ainsi jusqu'à avoir atteint la vitesse minimale.

MU-5.3.3 Configuration gestion EOC

Qu'est-ce que l'EOC?

Les unités SHDSL peuvent communiquer entre elles par le biais du Embedded Operations Channel (EOC). Par exemple, le Routeur Telindus 1421 SHDSL peut envoyer les types de demandes EOC suivants:

- inventaire, pour obtenir des informations (fabricant, version, etc.) sur l'unité SHDSL distante,
- activer / désactiver les boucles de retour du réseau sur l'unité SHDSL distante,
- demander au CPE d'indiquer les statistiques ou les informations de défaillance (marge SNR, atténuation de boucle, nombre d'erreurs CRC, etc.).

Les messages EOC sont définis dans G.991.2 pour assurer l'interopérabilité des systèmes.

Configuration gestion EOC

Utilisez l'attribut telindus1421Router/wanInterface/line/eocHandling pour définir la gestion des messages EOC.

L'attribut eocHandling a les valeurs suivantes:

Valeur	Description
none	Le Routeur Telindus 1421 SHDSL lui-même n'envoie pas de demandes EOC. Toutefois, le Routeur Telindus 1421 SHDSL répond aux demandes EOC qu'il reçoit.
discovery inventory info	Le Routeur Telindus 1421 SHDSL “scanne” la ligne SHDSL. Pour chaque unité qu'il découvre, il ajoute un objet dans l'arborescence. Reportez-vous à Découverte d'unités sur la ligne SHDSL. Ensuite, le Routeur Telindus 1421 SHDSL récupère les informations de ces unités et les affiche dans les objets correspondants. Les informations récupérées dépendent en fait du réglage de l'attribut eocHandling. Reportez-vous à MU-5.3.4 - Information EOC récupérée page 69.
alarmConfiguration	Dans ce cas aussi, le Routeur Telindus 1421 SHDSL “scanne” la ligne SHDSL, ajoute les objets à l'arborescence et récupère les informations des unités. Reportez-vous à Découverte d'unités sur la ligne SHDSL et MU-5.3.4 - Information EOC récupérée page 69. De plus, l'unité centrale [1] SHDSL force l'unité SHDSL distante [2] à utiliser les seuils d'alarme de liaison lineAttenuationOn et signalNoiseOn tels que configurés sur l'unité centrale. En d'autres termes, les réglages de lineAttenuationOn et signalNoiseOn sur l'unité centrale sont prioritaires sur ceux de l'unité distante.

1. L'unité centrale est l'unité sur laquelle l'attribut channel est réglé sur central.
2. L'unité distante est l'unité sur laquelle l'attribut channel est réglé sur remote.

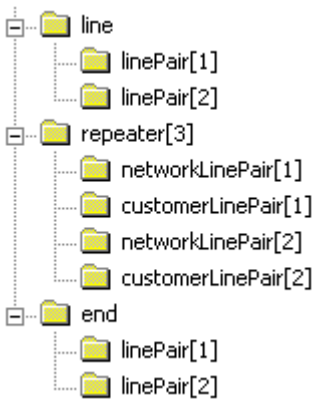
Découverte d'unités sur la ligne SHDSL

Lorsque vous modifiez l'attribut eocHandling pour le faire passer de none à une quelconque autre valeur, le Routeur Telindus 1421 SHDSL commence à "scanner" la ligne SHDSL pour déterminer quelles unités sont présentes entre lui-même et sa contrepartie distante.

Une fois ce scan terminé, certains nouveaux objets sont ajoutés dans l'arborescence [1] au même niveau que l'objet line:

- Si un ou plusieurs répéteurs sont présents sur la ligne SHDSL, un objet repeater[ ] est ajouté pour chacun d'entre eux.
- Pour la partie distante, un objet end est ajouté.

Par exemple, supposons que vous ayez une liaison avec un Crocus SHDSL comme unité centrale, un Routeur Telindus 1421 SHDSL comme unité distante et un répéteur Crocus SHDSL entre les deux. Supposons que vous régliez l'attribut eocHandling sur discovery. Dans ce cas, un objet repeater[ ] et un objet end sont ajoutés à l'arborescence, comme le montre la figure.



1. Il peut s'écouler jusqu'à 5 minutes avant que ces nouveaux objets apparaissent dans l'arborescence.

MU-5.3.4 Information EOC récupérée

Comme nous l'avons vu dans MU-5.3.3 - Configuration gestion EOC page 67, les informations récupérées de l'unité SHDSL distante par le canal EOC dépendent du réglage de l'attribut eocHandling.

Cette section donne un aperçu des cas dans lesquels les informations sont récupérées:

- Information d'état EOC page 70
- Information de performance EOC page 71
- Information d'alarme EOC page 72

Information d'état EOC		**L'attribut ou l'élément affiche-t-il des informations pertinentes lorsque eocHandling est réglé sur …?**				
Objet telindus1421Router/ ...	**Attribut (Elément)**	**none**	**discovery**	**inventory**	**info**	**alarmConfiguration**
ligne	eocAlarmThresholds (lineAttenuation, signalNoise)	Non. La valeur est toujours 0.0.	• Sur le central[1]: oui. Les valeurs sont celles spécifiées dans l'attribut linkAlarmThresholds. • Sur le modem distant[2]: non. La valeur est toujours 0.0.			Oui. Les valeurs sont celles spécifiées dans l'attribut linkAlarmThresholds sur l'unité centrale [3].
	numDiscoveredRepeaters	Oui.				
répéteur [ ] ou fin.	vendorId (countryCode, providerCode, vendorSpecific)	Aucun objet repeater[ ] ni end n'est créé.	Oui.			
	vendorModel		Non.	Oui.		
	vendorSerial		Non.	Oui.		
	vendorSoftVersion		Non.	Oui.		
	eocSoftVersion		Oui.			
	shdslVersion		Oui.			
	eocState		Oui.			
	eocAlarmThresholds (lineAttenuation, signalNoise)		Non. La valeur est toujours 0.0.		Oui. Les valeurs sont celles spécifiées dans l'attribut linkAlarmThresholds sur l'unité distante.	Oui. Les valeurs sont celles spécifiées dans l'attribut linkAlarmThresholds sur l'unité centrale.
répéteur [ ]/linePair[ ] ou end/linePair[ ]	lineAttenuation	Aucun objet repeater[ ] ni end n'est créé.	Non. La valeur est toujours 0.0.		Oui. Les valeurs sont l'atténuation effective de ligne et le bruit du signal tels que mesurés sur l'unité distante.	
	signalNoise					

1. L'unité centrale est l'unité sur laquelle l'attribut channel est réglé sur central.

Information de performance EOC		**L'attribut ou l'élément affiche-t-il des informations pertinentes lorsque eocHandling est réglé sur …?**				
Objet telindus1421Router/ ...	**Attribut**	**none**	**discovery**	**inventory**	**info**	**alarmConfiguration**
répéteur [ ]/linePair[ ] ou end/linePair[ ]	lineParameters	Aucun objet repeater[ ] ni end n'est créé.	Non. La valeur est toujours 0.0.		Oui. Les valeurs sont les mêmes que celles de l'unité distante. Notez que dans ce cas, le sysUpTime n'est pas la durée écoulée depuis le dernier démarrage à froid, mais la durée écoulée depuis la création de l'objet repeater[ ] ou end.	
	performance					
	h2LineParameters					
	h2Performance					
	h24LineParameters					
	h24Performance					
	d7LineParameters					
	d7Performance					

Information d'alarme EOC		**L'attribut ou l'élément affiche-t-il des informations pertinentes lorsque eocHandling est réglé sur …?**				
Objet telindus1421Router/ ...	**Attribut**	**none**	**discovery**	**inventory**	**info**	**alarmConfiguration**
line/linePair[ ]	lineAttenuation	Les seuils tels que configurés dans l'attribut linkAlarmThresholds sur l'unité locale sont utilisés pour générer les alarmes.				Les seuils tels que configurés dans l'attribut linkAlarmThresholds sur l'unité [1]centrale sont utilisés pour générer les alarmes[2].
	signalNoise					
répéteur [ ]/linePair[ ] ou end/linePair[ ]	lineAttenuation	Aucun objet repeater[ ] ni end n'est créé.	Aucune alarme n'est générée.		Les seuils tels que configurés dans l'attribut linkAlarmThresholds sur l'unité locale sont utilisés pour générer les alarmes.	Les seuils tels que configurés dans l'attribut linkAlarmThresholds sur l'unité centrale sont utilisés pour générer les alarmes.
	signalNoise					
	errSecExceeded					Les seuils tels que configurés dans l'attribut linkAlarmThresholds sur l'unité locale sont utilisés pour générer les alarmes.
	sevErrSecExceeded					

1. L'unité centrale est l'unité sur laquelle l'attribut channel est réglé sur central.
2. Reportez-vous à MU-5.3.3 - Configuration gestion EOC page 67 pour de plus amples informations sur la valeur alarmConfiguration.

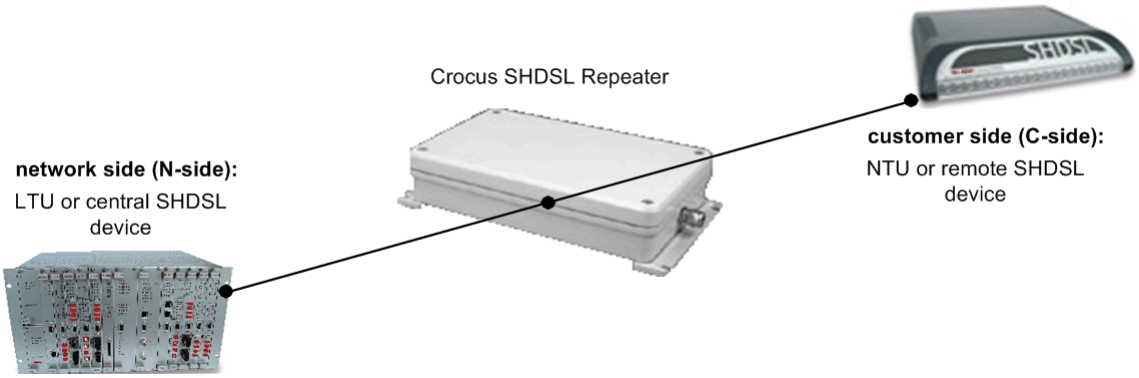
MU-5.3.5 Sécurité d'alimentation

Le Routeur Telindus 1421 SHDSL dispose de la sécurité d'alimentation. La sécurité d'alimentation fait partie de la recommandation ITU-T G.991.2 SHDSL. Elle réduit le niveau de puissance de transmission maximum si l'état de la ligne est suffisamment bon pour fonctionner à un niveau plus bas.

La sécurité d'alimentation se fait par défaut (aucun attribut de configuration). Lors de l'établissement de la liaison ITU-T G.994.1, les deux côtés de la ligne conviennent mutuellement du niveau de transmission. Le niveau de transmission est abaissé entre 0 et 6 dB, par paliers de 1dB.

MU-5.3.6 Utilisation d'un répéteur sur la ligne SHDSL

Un répéteur Crocus SHDSL vous permet d'accroître la distance entre les unités SHDSL centrale et distante.



Le répéteur Crocus SHDSL actuel ne peut fonctionner qu'en mode plésiochrone sur la ligne SHDSL. Reportez-vous à telindus1421Router/wanInterface/line/timingMode page 64.

MU-5.3.7 Compatibilité avec d'autres unités SHDSL

Le Routeur Telindus 1421 SHDSL peut être utilisé en combinaison avec d'autres unités SHDSL (Telindus). Le document intitulé “Interopérabilité des produits SHDSL Telindus” (PDF) donne un aperçu de cette interopérabilité.

MU-5.4 Configuration des mots de passe

Cette section vous indique comment créer une liste de mots de passe avec des niveaux d'accès associés dans la table de sécurité. Elle explique également comment corriger la table de sécurité en cas d'erreur ou en cas d'oubli du mot de passe. De plus, cette section vous montre comment entrer les mots de passe dans les différents outils de maintenance.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-5.4.1 - Création de mots de passe dans la table de sécurité page 75
- MU-5.4.2 - Entrée des mots de passe dans les différents outils de gestion page 75

MU-5.4.1 Création de mots de passe dans la table de sécurité

Pour éviter un accès non autorisé au Routeur Telindus 1421 SHDSL et au réseau, vous pouvez créer une liste de mots de passe avec des niveaux d'accès associés dans la table de sécurité. Pour ce faire, utilisez l'attribut security. Reportez-vous à telindus1421Router/security page 15.

MU-5.4.2 Entrée des mots de passe dans les différents outils de gestion

Maintenant que vous avez créé une liste de mots de passe dans le Routeur Telindus 1421 SHDSL, vous devez entrer ces mots de passe chaque fois que vous souhaitez accéder au Routeur Telindus 1421 SHDSL avec l'un des outils de gestion ou de maintenance.

Le tableau suivant explique comment entrer les mots de passe dans les différents outils de gestion ou de maintenance:

Outil de maintenance ou de gestion	**Comment entrer le mot de passe?**
TMA	Entrez le mot de passe dans la fenêtre *Connect…*.
TMA CLI, TMA pour HP OpenView et TMA Element Management	Utilisez l'application *TmaUserConf.exe* pour créer un utilisateur TMA et affecter un mot de passe à cet utilisateur. Le mot de passe doit correspondre à un mot de passe configuré dans l'unité. Reportez-vous au manuel TMA CLI (PDF), au manuel TMA pour HP OpenView (PDF) ou au manuel TMA Element Management (PDF/CHM) pour de plus amples informations.
CLI	Vous êtes invité à entrer le mot de passe lorsque la session débute.
ATWIN	Vous êtes invité à entrer le mot de passe lorsque la session CLI débute. Vous pouvez ensuite démarrer la session ATWIN.
Interface web	Vous êtes invité à entrer le mot de passe lorsque la session débute.
SNMP	Définissez le mot de passe comme une chaîne commune. Si aucun mot de passe n'est défini, vous pouvez utiliser n'importe quelle chaîne comme chaîne commune.
TML	Entrez le mot de passe après le nom du fichier de destination. Séparez le mot de passe et le nom du fichier par un '?'. Exemple: `tml -fsourcefile@destinationfile?pwd`
(T)FTP	Entrez le mot de passe après le nom du fichier de destination. Séparez le mot de passe et le nom du fichier par un '?'. Exemple: `entrez sourcefile destinationfile?pwd`

MU-5.5 Exécution des actions de configuration

Cette section vous montre comment exécuter les actions sur la configuration. Le tableau suivant donne un aperçu de ce chapitre:

- MU-5.5.1 - Quels sont les différents types de configuration? page 77
- MU-5.5.2 - Activation de la configuration page 78
- MU-5.5.3 - Chargement de la configuration par défaut page 78
- MU-5.5.4 - Chargement de la configuration par défaut en utilisant un commutateur DIP page 79

MU-5.5.1 Quels sont les différents types de configuration?

Cette section explique les différents types de configuration présents dans le Routeur Telindus 1421 SHDSL.

Quels sont les types de configuration?

Trois types de configuration sont présents dans le Routeur Telindus 1421 SHDSL:

- la configuration non active
- la configuration active
- la configuration par défaut

Explication des types de configuration

Lors de la configuration du Routeur Telindus 1421 SHDSL, il se produit la chose suivante:

Phase	Action	Résultat
1	Connectez l'ordinateur utilisant l'outil de maintenance au Routeur Telindus 1421 SHDSL.	La configuration non active apparaît à l'écran.
2	Modifiez la configuration non active.	Ces modifications n'ont aucune influence immédiate sur la configuration active actuellement utilisée par le Routeur Telindus 1421 SHDSL.
3	Des modifications sont entreprises sur la configuration non active.	La configuration non active doit être activée.
4	Dans le cas d'un … • TMA, cliquez sur le bouton TMA *Send all attributes to device*: . • tout autre outil de maintenance que le TMA basé sur l'interface utilisateur graphique (p. ex. ATWIN, CLI, Web Interface, EasyConnect terminal, TMA CLI), puis exécutez l'action Activate Configuration.	La configuration non active devient la configuration active.

Quelles sont les actions de configuration?

Vous pouvez exécuter les actions suivantes sur la configuration:

- telindus1421Router/Activate Configuration page 17
- telindus1421Router/Load Default Configuration page 17
- telindus1421Router/Load Saved Configuration page 17

MU-5.5.2 Activation de la configuration

Comme le montre la section MU-5.5.1 - Quels sont les différents types de configuration? page 77, après avoir configuré le Routeur Telindus 1421 SHDSL vous devez activer les changements de configuration entrepris.

Dans le cas d'un …

- TMA, cliquez sur le bouton TMA *Send all attributes to device*: .
- tout autre outil de maintenance que le TMA basé sur l'interface utilisateur graphique (p. ex. ATWIN, CLI, Web Interface, EasyConnect terminal, TMA CLI), puis exécutez l'action Activate Configuration.

MU-5.5.3 Chargement de la configuration par défaut

Lorsque vous installez le Routeur Telindus 1421 SHDSL pour la première fois, l'ensemble des attributs de configuration sont réglés sur leurs valeurs par défaut. Si le Routeur Telindus 1421 SHDSL a déjà été configuré, mais que vous souhaitez recommencer depuis le départ, utilisez cette action pour revenir à la configuration par défaut.

Vous pouvez charger la configuration par défaut en utilisant *Load Default Configuration* …

- Reportez-vous à telindus1421Router/Load Default Configuration page 17.
- Commutateur DIP Reportez-vous à MU-5.5.4 - Chargement de la configuration par défaut en utilisant un commutateur DIP page 79.

MU-5.5.4 Chargement de la configuration par défaut en utilisant un commutateur DIP

Les procédures suivantes vous montrent comment charger la configuration par défaut en utilisant le commutateur DIP *Load Default Configuration* sur la carte du Routeur Telindus 1421 SHDSL:

Etape	Action
1	Déconnectez l'alimentation et ouvrez le boîtier comme décrit dans MU-3.3 - Ouverture et fermeture du boîtier page 29.
2	Placez le commutateur DIP *Load default configuration* sur *off*. Reportez-vous à MU-3.1 - La carte mère du Routeur Telindus 1421 SHDSL page 27 pour localiser cette réglette de commutateurs DIP.
3	Replacez le capot sans serrer les vis et reconnectez l'alimentation. ⇒Le Routeur Telindus 1421 SHDSL se réinitialise et charge la configuration par défaut.
4	Activez la configuration par défaut ainsi chargée: 1. Ouvrez une session TMA sur le Routeur Telindus 1421 SHDSL. Reportez-vous à MU-4.1 - Maintenance du Routeur Telindus 1421 SHDSL avec TMA page 31. 2. Exécutez l'action Activate Configuration.
5	Déconnectez l'alimentation et ouvrez le boîtier.
6	Réinitialisez le commutateur DIP *Load default configuration* sur *on*.
7	Replacez correctement le capot comme décrit dans MU-3.3 - Ouverture et fermeture du boîtier page 29 et reconnectez l'alimentation.

Réinitialisez le Routeur Telindus 1421 SHDSL après avoir modifié les commutateurs DIP.

MU-5.6 Configuration des principales fonctions du Routeur Telindus 1421 SHDSL

La liste qui suit vous indique où trouver une présentation et une configuration de base des principales fonctions du Routeur Telindus 1421 SHDSL:

- MU-6 - Configuration des protocoles d'encapsulation page 82
- MU-7 - Configuration d'acheminement page 148
- MU-8 - Configuration du pontage page 224
- MU-9 - Configuration des fonctions complémentaires page 252 (p. ex. configuration DHCP, listes d'accès, VLAN, tunnels L2TP tunnels, etc.)

MU-5.7 Dépistage des erreurs Routeur Telindus 1421 SHDSL

Si vous rencontrez des problèmes lors de l'installation, de la configuration ou du fonctionnement du Routeur Telindus 1421 SHDSL, vérifiez les points suivants:

Contrôle	Description
alimentation	Le Routeur Telindus 1421 SHDSL est-il alimenté correctement?
connexions	Tous les câbles nécessaires sont-ils connectés au Routeur Telindus 1421 SHDSL? Sont-ils connectés aux connecteurs corrects du Routeur Telindus 1421 SHDSL? Sont-ils correctement connectés? Avez-vous utilisé les câbles corrects (droits, croisés, …)? Reportez-vous à MU-2.6 - Connexion Routeur Telindus 1421 SHDSL page 17.
autres unités	Les unités connectées au Routeur Telindus 1421 SHDSL fonctionnent-elles correctement (sont-elles alimentées, opérationnelles, …)?
Diodes	Qu'indiquent les diodes du Routeur Telindus 1421 SHDSL? Indiquent-elles une défaillance? Reportez-vous à MU-2.7 - Témoins à DEL du panneau avant page 21.
messages	Quels sont les messages affichés dans la table messages? Cette table affiche des messages informatifs et d'erreur. Reportez-vous à telindus1421Router/messages page 177.
status	Qu'indiquent les attributs d'état du Routeur Telindus 1421 SHDSL? Quel est l'état des différentes interfaces (marche, arrêt, test, …)? Reportez-vous à MR-2 - Status attributes page 168.
performance	Qu'indiquent les attributs de performance du Routeur Telindus 1421 SHDSL? Quelles sont les performances des différentes interfaces (les données passent-elles l'interface, l'interface fonctionne-t-elle ou non, quand est-elle passée en ordre de marche, …)? Reportez-vous à MR-3 - Performance attributes page 278.
alarmes	Qu'indiquent les attributs d'alarme du Routeur Telindus 1421 SHDSL? Quel est l'état d'alarme des différentes interfaces (liaison interrompue, erreur, …)? Reportez-vous à MR-4 - Alarm attributes page 334.

MU-6 Configuration des protocoles d'encapsulation

Ce chapitre présente les protocoles d'encapsulation et répertorie les attributs que vous pouvez utiliser pour configurer ces protocoles.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-6.1 - Sélection d'un protocole d'encapsulation page 83
- MU-6.2 - Configuration d'encapsulation ATM page 84
- MU-6.3 - Configuration d'encapsulation de Frame Relay page 105
- MU-6.4 - Configuration d'encapsulation PPP page 121
- MU-6.5 - Configuration d'encapsulation HDLC page 144
- MU-6.6 - Configuration d'un test d'erreur page 146

Reportez-vous au Manuel de référence pour un aperçu complet des attributs du Routeur Telindus 1421 SHDSL.

MU-6.1 Sélection d'un protocole d'encapsulation

Sélectionnez d'abord le protocole d'encapsulation que vous souhaitez utiliser. Pour ce faire, utilisez l'attribut encapsulation. Reportez-vous à telindus1421Router/wanInterface/encapsulation page 30.

Une fois sélectionné le protocole d'encapsulation, vous pouvez l'adapter comme cela est décrit dans ce chapitre.

MU-6.2 Configuration d'encapsulation ATM

Cette section présente le protocole d'encapsulation ATM et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-6.2.1 - Introduction à ATM page 85
- MU-6.2.2 - Configuration d'ATM PVC page 91
- MU-6.2.3 - Obtention automatique d'adresses IP dans ATM page 93
- MU-6.2.4 - Configuration d'adresses IP dans ATM page 94
- MU-6.2.5 - Configuration VPI et VCI page 95
- MU-6.2.6 - Configuration UBR page 96
- MU-6.2.7 - Redistribution de largeur de bande ATM PVC page 97
- MU-6.2.8 - Configuration Ethernet/IP ponté/acheminé sur ATM (RFC 2684) page 100
- MU-6.2.9 - Configuration d'IP classique IP (IPoA) page 101
- MU-6.2.10 - Configuration PPP sur ATM (PPPoA) page 102
- MU-6.2.11 - Configuration PPP sur Ethernet (PPPoE) page 103
- MU-6.2.12 - Configuration ATM sur une interface G703 page 104

MU-6.2.1 Introduction à ATM

Qu'est-ce que l'ATM?

ATM est une technologie de commutation de cellule et de multiplexage qui combine les avantages de la commutation de circuit (capacité garantie et retard de transmission constant) à ceux de la commutation par paquets (flexibilité et efficacité du trafic intermittent). Elle offre une largeur de bande étalonnable. Du fait de sa nature asynchrone, l'ATM est plus efficace que les technologies synchrones telles que la TDM (multiplexage par division de temps).

Avec la TDM, chaque utilisateur se voit attribuer un intervalle de temps et aucune autre station ne peut émettre durant cet intervalle. Si une station a d'importantes quantités de données à envoyer, elle ne peut le faire que dans cet intervalle de temps, mais si tous les autres intervalles sont inoccupés. Toutefois, si une station n'a rien à transmettre lorsque son intervalle de temps survient, ce dernier est envoyé vide et est ainsi "gâché". L'ATM étant asynchrone, les intervalles de temps sont disponibles sur demande, avec des informations identifiant la source de la transmission contenues dans l'en-tête de chaque cellule ATM.

Qu'est-ce que VPI et VCI?

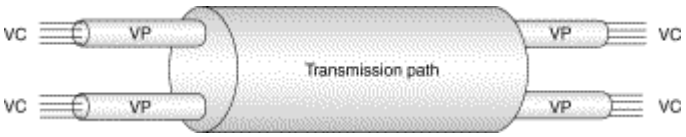
Les réseaux ATM sont orientés en fonction de la connexion, ce qui signifie qu'un canal virtuel doit être configuré sur le réseau ATM avant tout transfert de données. (Un canal virtuel est grosso modo équivalent à un circuit virtuel permanent, ou PVC.)

Il existe deux types de connexions ATM:

- les trajets virtuels, identifiés par des identificateurs de trajet virtuel (VPI).
- les canaux virtuels, identifiés par la combinaison d'un VPI et d'un VCI.

Un trajet virtuel est un ensemble de canaux virtuels qui sont tous commutés de manière transparente sur le réseau ATM en fonction de leur VPI commun. Toutefois, l'ensemble des VPI et VCI n'ont qu'une signification locale sur une liaison spécifique et sont redéfinis, selon le cas, lors de chaque commutation.

Un trajet de transmission est le support physique qui transporte les canaux virtuels et les trajets virtuels. La figure qui suit illustre comment les VC se groupent pour créer des VP, qui, à leur tour, traversent le support ou le trajet de transmission.



Que sont les couches ATM?

Le modèle de référence ATM se compose des couches ATM suivantes:

<table>
<tr><th>Couche</th><th>Description</th></tr>
<tr><td>couche physique</td><td>Analogue à la couche physique d'un modèle de référence OSI, la couche physique ATM gère la transmission en fonction du support.</td></tr>
<tr><td>Couche ATM</td><td>Combinée avec la couche d'adaptation ATM, la couche ATM est à peu près analogue à la couche de liaison de données du modèle de référence OSI. La couche ATM est responsable du partage simultané des circuits virtuels sur une liaison physique (multiplexage de cellules) et de la transmission des cellules dans le réseau ATM (relais de cellules). Pour ce faire, elle utilise les informations VPI et VCI contenues dans l'en-tête de chaque cellule ATM.</td></tr>
<tr><td>Couche d'adaptation ATM (AAL)</td><td>Combinée avec la couche ATM, l'AAL est à peu près analogue à la couche de liaison de données du modèle OSI. L'AAL est responsable de l'isolation des protocoles de couche supérieure à partir des détails des processus ATM. La couche d'adaptation prépare les données utilisateurs en vue de leur conversion en cellules et segmente les données en paquets de cellules de 48 octets.

Actuellement, les quatre types d'AAL recommandés par l'ITU-T sont AAL1, AAL2, AAL3/4, et AAL5:

<table>
<tr><th>AAL</th><th>Description</th></tr>
<tr><td>AAL1</td><td>AAL1 est utilisé pour des services orientés connexion, sensibles à la temporisation, et qui nécessitent des vitesses binaires constantes, tels que la vidéo non comprimée et d'autres trafics isochrones.</td></tr>
<tr><td>AAL2</td><td>AAL2 est utilisé pour des services orientés connexion qui supportent une vitesse binaire variable, tels que certains trafics vidéo et vocaux isochrones.</td></tr>
<tr><td>AAL3/4</td><td>AAL3/4 (combinaison de deux couches d'adaptation initialement distincte) supporte des liaisons sans connexion et orientées connexion, mais est essentiellement utilisée pour la transmission de paquets SMDS sur les réseaux ATM.</td></tr>
<tr><td>AAL5</td><td>AAL5 supporte les services VBR orientés connexion et est utilisé essentiellement pour le transfert d'IP classiques sur le trafic ATM et LANE. AAL5 utilise SEAL et est la moins complexe de toutes les recommandations AAL actuelles. Il offre une faible largeur de bande et des besoins de traitement plus simples en échange d'une capacité de largeur de bande réduite et d'une capacité de recouvrement d'erreur.</td></tr>
</table>
</td></tr>
<tr><td>couches supérieures</td><td>Enfin, les couches supérieures résidant au-dessus de l'AAL acceptent les données utilisateur, les disposent en paquets et les transmettent à l'AAL.</td></tr>
</table>

Que sont les catégories de services ATM?

La spécification de gestion de trafic version 4.0 définit cinq catégories de service ATM qui décrivent le trafic transmis par les utilisateurs sur un réseau et la qualité de service (QoS) qu'un réseau a besoin de fournir pour ce trafic. Les cinq catégories de service sont:

- Vitesse binaire constante (CBR)
- Vitesse binaire variable temps non réel (VBR-nrt)
- Vitesse binaire variable temps réel (VBR-nrt)
- Vitesse binaire disponible (CBR)
- Vitesse binaire non spécifiée (CBR)

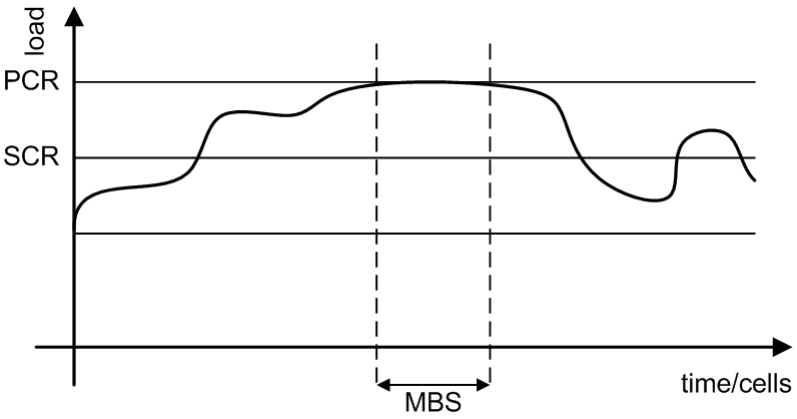
Le Routeur Telindus 1421 SHDSL supporte UBR.

Quels sont les paramètres de trafic des catégories de service ATM?

Les paramètres de trafic avec lesquels vous pouvez configurer les catégories de services ATM sont:

paramètre de trafic	**Description**
PCR	Le Peak Cell Rate (PCR) est la vitesse maximale à laquelle vous pouvez escompter transmettre les données. De toute évidence, le PCR maximum possible est la vitesse physique du circuit d'accès du client dans le fournisseur de services ATM.
SCR	Le Sustainable Cell Rate (SCR) est la vitesse supportée à laquelle vous pouvez escompter transmettre les données. Le SCR est la largeur de bande réelle d'un PVC, et non la vitesse de trafic moyenne sur le long terme.
MBS	Le Maximum Burst Size (MBS) est le temps ou la durée pendant lequel le routeur envoie avec le PCR (en d'autres termes, il indique combien de cellules peuvent être transmises à la vitesse PCR). Calculez ce temps en secondes en utilisant la formule suivante: T = (cellules émises x 424 bits par cellule) / (PCR - SCR) MBS accepte les piques temporaires ou les pointes de courte durée dans le motif de trafic. Par exemple, un MBS de 100 cellules permet un pique de trois trames Ethernet de taille MTU. Il est important de factoriser des piques de durée plus longue dans le SCR.

La figure qui suit montre la relation entre PCR, SCR et MBS:



Qu'est-ce que l'UBR?

Le Unspecified Bit Rate (UBR) est un service d'affectation de largeur de bande qui ne garantit aucun niveau de débit et utilise uniquement les largeurs de bande existantes. UBR est conçu pour des applications en temps non réel qui ne nécessitent pas de liaison maximale sur le retard de transfert ou le rapport cellule-perte.

Avantages	• UBR offre un degré plus élevé de multiplexage statistique en ne réservant aucune largeur de bande minimale par PVC. Les PVC utilisent la largeur de bande jusqu'au PCR configuré lorsque cela est possible. • L'UBR modélise le meilleur service normalement fourni par l'internet. Adapté à des applications tolérant une temporisation et ne nécessitant aucune réponse en temps réel. Les exemples sont les e-mail, la transmission par fax, les transferts de fichiers, telnet, LAN et les interconnexions de bureaux distants. De telles applications ne sont pas sensibles au retard, mais à la perte de cellules.
Inconvénients	Les PVC UBR peuvent subir un grand nombre de pertes de cellules ou un fort retard de transfert de cellules lorsque les cellules passent de l'unité source à l'unité de destination.

Le seul paramètre de trafic que vous devez configurer en cas d'UBR est le PCR. Le PCR fournit seulement une indication d'une limitation de largeur de bande physique au sein d'un PVC.

Qu'est-ce que le multi-protocol sur ATM (MpoA)?

Comme son nom l'indique, l'encapsulation multi-protocole sur ATM est un mécanisme de transport de données autre que juste les IP. Plusieurs protocoles différents peuvent être utilisés sur l' ATM:

- Ethernet/IP ponté/acheminé sur ATM (anciennement RFC 1483, désormais RFC 2684). Ce protocole fait apparaître le routeur comme une unité LAN pour le système d'exploitation.
- IP sur ATM (IPoA, RFC 1577, similaire à RFC 2684). Ce protocole fait également apparaître le routeur comme une unité LAN pour le système d'exploitation.
- Point to Point Protocol sur ATM (PPPoA, RFC 2364). PPP assure la mise en route de sessions, l'authentification de l'utilisateur (login), et l'encapsulation des protocoles de couche supérieure tels que IP. L'emploi de PPP fait apparaître le routeur comme une unité de numérotation pour le système d'exploitation.
- Point to Point Protocol sur Ethernet (PPPoE, RFC 2516). Ce protocole fait apparaître le routeur comme une unité LAN pour le système d'exploitation. Il permet à plusieurs unités présentes sur un Ethernet de partager une connexion commune au réseau distant (l'internet).

Quels sont les mécanismes d'encapsulation multi-protocole sur ATM?

Comme nous l'avons vu précédemment, vous pouvez encapsuler plusieurs protocole dans ATM. Les mécanismes pour ce faire sont les suivants:

mécanisme d'encapsulation MPoA	**Description**
encapsulation Logical Link Control (LLC)	Avec cette méthode, plusieurs types de protocoles peuvent être transportés sur une seule connexion avec le type de paquet encapsulé identifiées par un en-tête standard LLC/SNAP.
Multiplexage de connexion virtuelle	Avec cette méthode, un seul protocole est transporté sur une connexion ATM, avec le type de protocole implicitement identifié lors de l'établissement de la connexion.

L'encapsulation LLC permet de supporter les protocoles acheminés et pontés. Avec ce format d'encapsulation, les PDU provenant de protocoles multiples peuvent être transportés par la même connexion virtuelle. Le type de protocole est indiqué dans l'en-tête SNAP du paquet. Par contraste, la méthode de multiplexage de connexion virtuelle permet le transport d'un seul protocole par connexion virtuelle.

La table qui suit donne un aperçu des mécanismes multi-protocole pouvant être utilisés pour l'encapsulation du protocole de couche supérieur.

Protocole de couche supérieure	**multiProtocolMech**
rfc2684	llcEncapsulation + vcMultiplexing
ppp	llcEncapsulation + vcMultiplexing
pppOverEthernet	llcEncapsulation

Qu'est-ce que PPPoA (RFC 2364)?

La couche d'adaptation PPP sur ATM 5 (AAL5) utilise AAL5 comme protocole tramé. Elle se fonde sur RFC 2684, fonctionnant en mode Logical Link Control Encapsulation ou en mode Virtual Connection Multiplexing. Une unité CPE (Customer Premises Equipment) encapsule la session PPP sur la base de ce RFC pour son transport sur la boucle xDSL et le DSLAM (Digital Subscriber Line Access Multiplexer).

Qu'est-ce que PPPoA (RFC 2516)?

Lorsque les clients déploient xDSL ils doivent supporter l'authentification PPP et l'autorisation sur une large base de CPE de pontage. PPPoE permet de connecter un réseau d'hôtes par une simple unité d'accès de pontage à un concentrateur d'accès distant.

Comme spécifié dans RFC 2516, PPPoE comporte deux étapes distinctes: une étape de découverte et une étape de session PPP. Lorsqu'un hôte initie une session PPPoE, il doit d'abord procéder à la découverte pour identifier le serveur capable de répondre à la demande du client, puis identifier l'adresse MAC Ethernet MAC du pair et établir une identification de session PPPoE. Alors que PPP définit une relation de pair à pair, la découverte est, par essence, une relation client-serveur.

Que sont les cellules OAM LoopBack (LB)?

Le protocole ATM dispose de cellules OAM LoopBack (LB). Elles sont utilisées pour vérifier si un canal/trajet virtuel est réellement actif ou pas. Cela peut se faire à deux niveaux:

- au niveau du trajet virtuel (VP) en utilisant les cellules OAM F4 LB . Les attributs de configuration correspondants se trouvent dans la table vp.
- au niveau du canal virtuel (VC) en utilisant les cellules OAM F5 LB. Les attributs de configuration correspondants se trouvent dans la table pvcTable.

Le Routeur Telindus 1421 SHDSL répond toujours aux cellules OAM LB reçues de l'unité pair ATM (segment et cellules de bout en bout). Toutefois, lorsque OAM LB est activé, le Routeur Telindus 1421 SHDSL envoie uniquement les cellules de demande bout en bout OAM LB.

Qu'est-ce que le CLP?

Le CLP (Cell Loss Priority) indique si la cellule doit être rejetée si elle rencontre un encombrement extrême lors de son transport dans le réseau. Si le bit CLP est égal à 1, la cellule doit être rejetée au bénéfice de cellules pour lesquelles le bit CLP est égal à 0.

Qu'est-ce que EFCI?

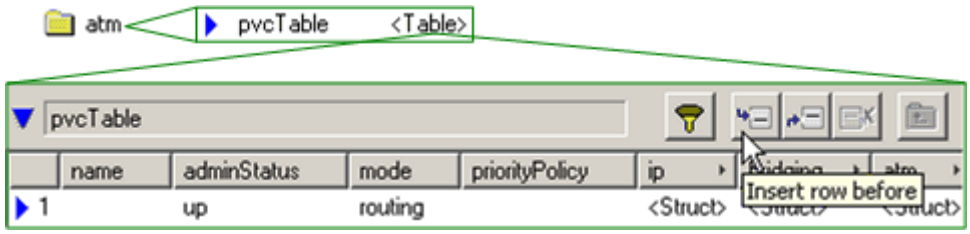
L'EFCI (Explicit Forward Congestion Indication) indique si une cellule contenant des données utilisateur a rencontré un encombrement lors de son transport dans le réseau.

MU-6.2.2 Configuration d'ATM PVC

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour la présentation.

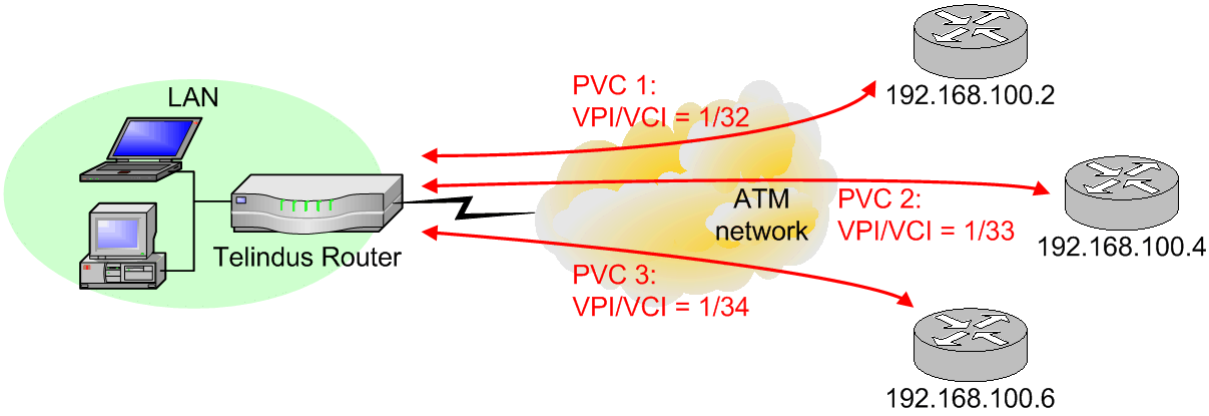
Dans un réseau ATM, vous pouvez configurer des PVC. Un PVC assure une connectibilité directe entre les sites. de cette manière, un PVC est similaire à une ligne louée. Un PVC garantit la disponibilité d'une connexion et ne nécessite aucune procédure de configuration d'appel entre les commutations ATM.

Pour configurer un ATM PVC, procédez de la manière suivante:

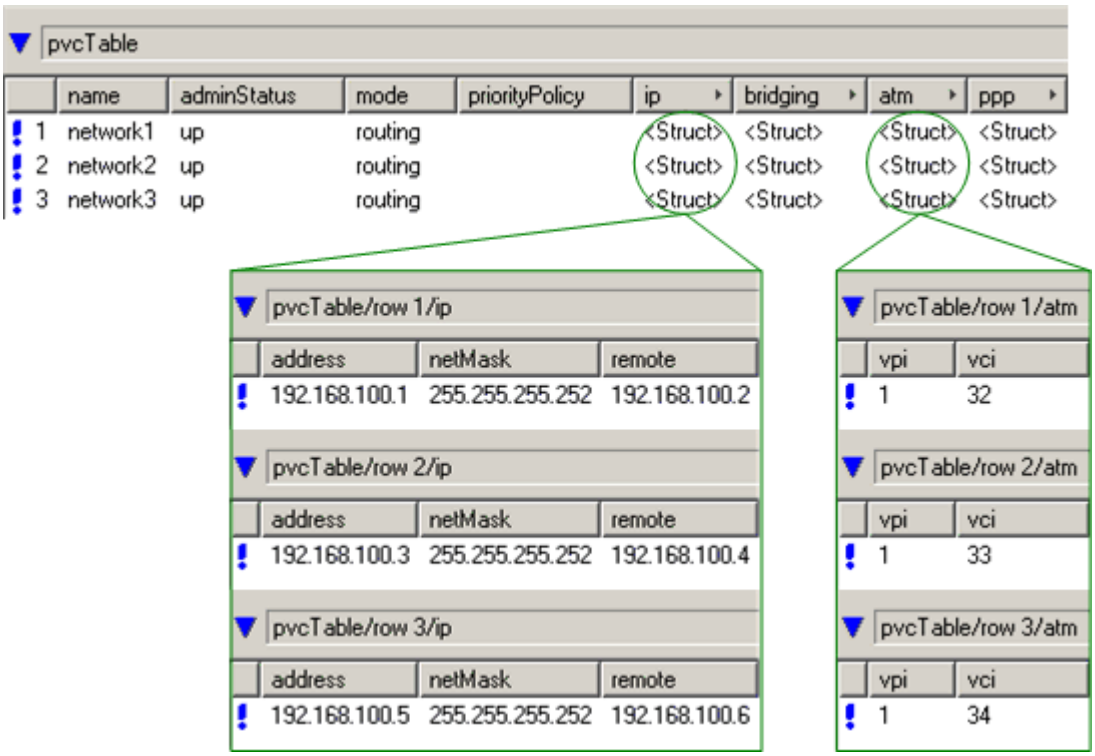
Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet atm, sélectionnez l'attribut pvcTable et ajoutez une ou plusieurs entrées à la table.  Utilisez cet attribut pour configurer les ATM PVC. Ajoutez une ligne au tableau pvcTable pour chaque ATM PVC que vous souhaitez créer.
2	Configurez les éléments de l'ATM PVC que vous venez de créer. Ces éléments sont: • name. Utilisez cet élément pour assigner un nom administratif à l'ATM PVC. • adminStatus. Utilisez cet élément pour activer (up) ou désactiver (down) l'ATM PVC. • mode. Utilisez cet élément pour déterminer si, pour l'ATM PVC correspondant, les paquets sont traités par le processus d'acheminement, de pontage ou les deux. • priorityPolicy. Utilisez cet élément pour appliquer une politique de priorité à l'ATM PVC. Reportez-vous à MU-7.8.7 - Application d'une politique de priorité sur une interface page 215 pour de plus amples informations. • ip. Utilisez cet élément pour configurer les paramètres de l'IP de l'ATM PVC. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour de plus amples informations. • bridging. Utilisez cet élément pour configurer les paramètres de pontage de l'ATM PVC si le PVC est en mode de pontage (c'est-à-dire si l'élément mode est réglé sur bridging). Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 pour de plus amples informations. • atm. Utilisez cet élément pour configurer les paramètres spécifiques de l'ATM sur l'ATM PVC. Reportez-vous à telindus1421Router/wanInterface/atm/pvcTable/atm page 36 pour de plus amples informations. • ppp. Utilisez cet élément pour configures les paramètres PPP de l'ATM PVC si vous souhaitez faire tourner PPP sur ATM. Reportez-vous à MR-1.5.3 - PPP configuration attributes page 52 pour une description détaillée des éléments de la structure ppp. Reportez-vous à telindus1421Router/wanInterface/atm/pvcTable page 34 pour une description détaillée de pvcTable.

Exemple – configuration ATM PVCs

La figure qui suit donne un exemple de segment Ethernet local connecté à trois réseaux différents par trois PVC différents:



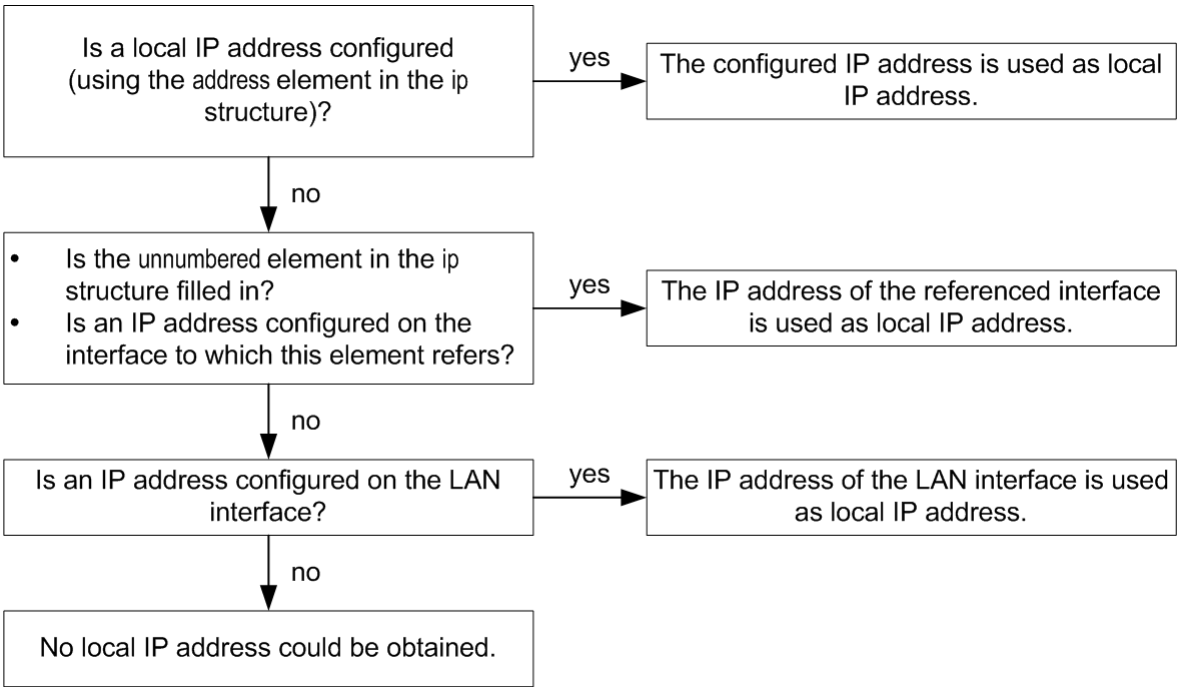
L'écran qui suit montre (en partie) la pvcTable de la configuration décrite dans la figure ci-dessus:



MU-6.2.3 Obtention automatique d'adresses IP dans ATM

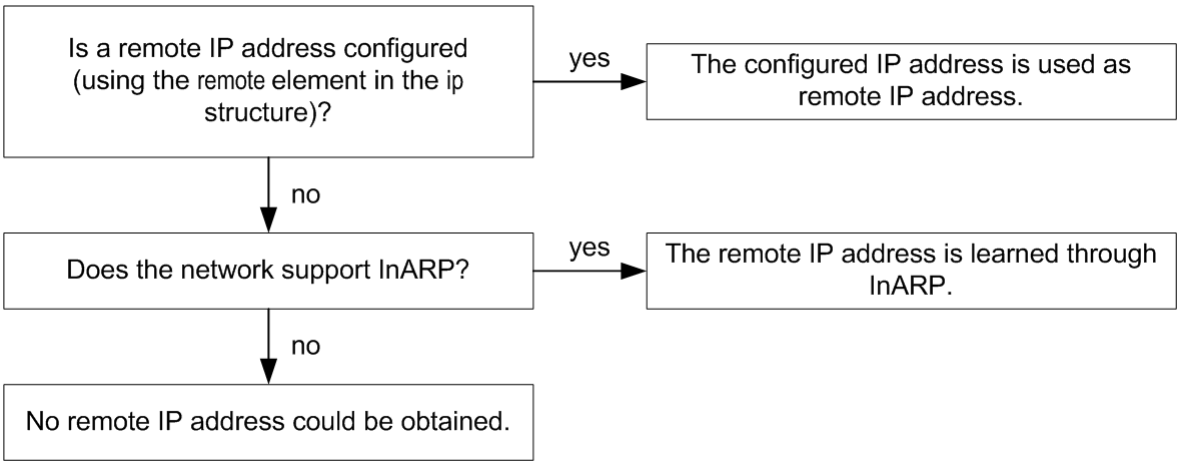
Obtention d'une adresse IP locale

Dans le cas de l'ATM, le Routeur Telindus 1421 SHDSL ne supporte pas actuellement une procédure automatique d'apprentissage de l'adresse IP locale d'un ATM PVC. Toutefois, si vous ne configurez pas l'adresse IP locale, l'adresse IP de l'interface LAN est utilisée.


Is a local IP address configured (using the address element in the ip structure)?
yes
The configured IP address is used as local IP address.
no
Is the unnumbered element in the ip structure filled in?
Is an IP address configured on the interface to which this element refers?
yes
The IP address of the referenced interface is used as local IP address.
no
Is an IP address configured on the LAN interface?
yes
The IP address of the LAN interface is used as local IP address.
no
No local IP address could be obtained.

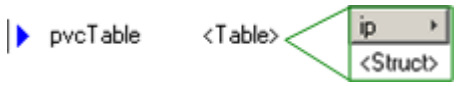
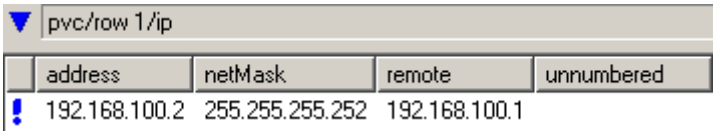
Obtention d'une adresse IP distante

Si le réseau ATM supporte le protocole InARP (Inverse Address Resolution Protocol), le Routeur Telindus 1421 SHDSL peut apprendre l'adresse IP distante d'un ATM PVC.


Is a remote IP address configured (using the remote element in the ip structure)?
yes
The configured IP address is used as remote IP address.
no
Does the network support InARP?
yes
The remote IP address is learned through InARP.
no
No remote IP address could be obtained.

MU-6.2.4 Configuration d'adresses IP dans ATM

Pour configurer des adresses IP dans un ATM PVC, procédez de la façon suivante:

Etape	Action
1	Dans pvcTable, sélectionnez la structure ip. 
2	Dans la structure ip, configurez les éléments suivants: • address. Utilisez cet élément pour affecter une adresse IP à l'extrémité locale de l'ATM PVC. • netMask. Utilisez cet élément pour affecter un masque de sous-écran IP à l'extrémité locale de l'ATM PVC. • remote. Utilisez cet élément pour affecter une adresse IP à l'extrémité distante de l'ATM PVC. • unnumbered. Si vous ne configurez pas explicitement une adresse IP locale pour un ATM PVC, vous pouvez utiliser cet élément pour "emprunter" l'adresse IP d'une autre interface pour laquelle une adresse IP est déjà configurée. 

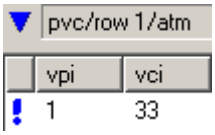
Reportez-vous au…

- MU-5.2.3 - Explication de la structure ip page 55 pour une description complète de la structure ip.
- Exemple – configuration ATM PVCs page 92 par exemple.

MU-6.2.5 Configuration VPI et VCI

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour une introduction à VPI et VCI.

Pour configurer VPI et VCI dans un ATM PVC, procédez de la façon suivante:

Etape	Action
1	Dans pvcTable, sélectionnez la structure atm.
2	Dans la structure atm, configurez les éléments suivants: • vpi. Utilisez cet élément pour déterminer le Virtual Path Identifier (VPI) de l'ATM PVC. • vci. Utilisez cet élément pour déterminer le Virtual Channel Identifier (VCI) de l'ATM PVC. 

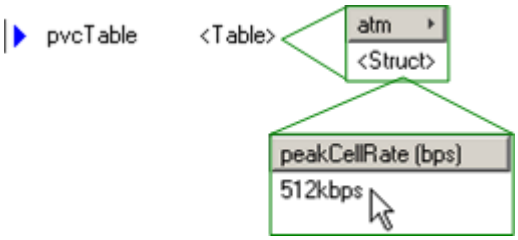
Reportez-vous au…

- telindus1421Router/wanInterface/atm/pvcTable/atm page 36 pour une description complète de la structure atm.
- Exemple – configuration ATM PVCs page 92 par exemple.

MU-6.2.6 Configuration UBR

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour une introduction à l'UBR et aux paramètres de trafic associés.

Pour configurer UBR dans un ATM PVC, procédez de la façon suivante:

Etape	Action
1	Dans pvcTable, sélectionnez la structure atm.
2	Dans la structure atm, configurez les paramètres de trafic UBR. Le seul paramètre que vous devez configurer en cas d'UBR est le PCR. Le PCR fournit seulement une indication d'une limitation de largeur de bande physique au sein d'un PVC. 

Reportez-vous au…

- telindus1421Router/wanInterface/atm/pvcTable/atm page 36 pour une description complète de la structure atm.
- MU-6.2.7 - Redistribution de largeur de bande ATM PVC page 97 pour des exemples.

Surdimensionnement du PCR

En cas de surdimension du PCR, le Routeur Telindus 1421 SHDSL peut (proportionellement) redistribuer la largeur de bande sur les différents PVC. Reportez-vous à MU-6.2.7 - Redistribution de largeur de bande ATM PVC page 97.

Lorsque vous dépassez la largeur de bande totale de la connexion physique, le Routeur Telindus 1421 SHDSL met les données en mémoire tampon. Toutefois, si les mémoires tampons du Routeur Telindus 1421 SHDSL sont remplies, elles doivent rejeter les données en “surplus”.

Remarque importante

Par définition, le PCR est la quantité spécifique de largeur de bande non garantie. Vous pouvez cependant définir une largeur de bande garantie en utilisant le PCR. Pour ce faire …

- ne surdimensionnez pas le PCR (c'est-à-dire ne laissez pas le total des PCR des PVC dépasser la largeur de bande de la connexion physique).
- ne réglez pas le PCR sur auto.

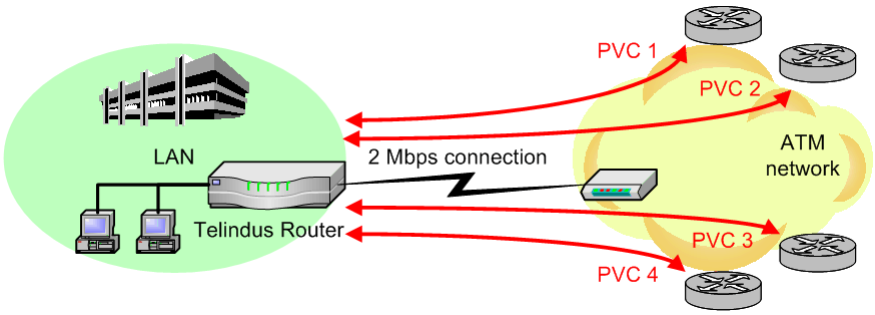
MU-6.2.7 Redistribution de largeur de bande ATM PVC

Dans ATM, la largeur de bande assignée à chaque PVC est recalculée à intervalles réguliers. Cela signifie qu'en fonction du trafic sur les PVC, le Routeur Telindus 1421 SHDSL peut (proportionnellement) diviser la largeur de bande par le nombre de PVC. Résultat, le surdimensionnement du PCR sur ATM n'est pas aussi grave que que surdimensionnement du CIR sur Frame Relay. Les exemples suivants l'expliquent de manière plus claire.

Exemples

Supposons que vous ayez une connexion physique de 2 Mbps vers le fournisseur de services ATM et que vous définissiez 4 PVC:

Les tables qui suivent illustrent certains scénarios possibles.



PCR = scénarios auto

Scénario:

	PCR configuré	Quantité de données envoyées	Largeur de bande assignée
PVC 1	auto	2048 kbps	512 kbps
PVC 2	auto	2048 kbps	512 kbps
PVC 3	auto	2048 kbps	512 kbps
PVC 4	auto	2048 kbps	512 kbps

⇒Tous les PCR étant réglés sur auto, chaque PVC tente d'obtenir une largeur de bande maximum. Donc, la largeur de bande totale disponible (2 Mbps) est répartie de manière égale entre quatre PVC.

Scénario:

	PCR configuré	Quantité de données envoyées	Largeur de bande assignée
PVC 1	auto	2048 kbps	512 kbps
PVC 2	auto	1024 kbps	512 kbps
PVC 3	auto	640 kbps	512 kbps
PVC 4	auto	512 kbps	512 kbps

⇒Tous les PCR étant réglés sur auto, chaque PVC tente d'obtenir une largeur de bande maximum. Donc, la largeur de bande totale disponible (2 Mbps) est répartie de manière égale entre quatre PVC. Dans ce scénario, la PVC 4 est la seule qui ait toutes ses données sur le réseau ATM.

Scénario:

	PCR configuré	**Quantité de données envoyées**	**Largeur de bande assignée**
PVC 1	auto	2048 kbps	2048 kbps
PVC 2	auto	0	0
PVC 3	auto	0	0
PVC 4	auto	0	0

⇒PVC 1 étant la seule à envoyer des données et son PCR étant réglé sur auto, elle obtient toute la largeur de bande disponibl (2 Mbps) et peut envoyer ses données à 2048 kbps.

PCR = scénarios fixes

Scénario:

	PCR configuré	**Quantité de données envoyées**	**Largeur de bande assignée**
PVC 1	1024 kbps	2048 kbps	1024 kbps
PVC 2	512 kbps	2048 kbps	512 kbps
PVC 3	448 kbps	2048 kbps	448 kbps
PVC 4	64 kbps	2048 kbps	64 kbps

⇒La somme des PCR étant égale à la largeur de bande totale disponible (2 Mbps), tous les PVC obtiennent la largeur de bande spécifiée dans leurs PCR respectifs.

Scénario:

	PCR configuré	**Quantité de données envoyées**	**Largeur de bande assignée**
PVC 1	2048 kbps	2048 kbps	1024 kbps
PVC 2	1024 kbps	2048 kbps	512 kbps
PVC 3	512 kbps	2048 kbps	256 kbps
PVC 4	512 kbps	2048 kbps	256 kbps

⇒Dans ce cas, les PCR des PVC sont surdimensionnés (c'est-à-dire que le total des PCR dépasse la largeur de bande de la connexion physique au réseau ATM). De plus, le montant total de données que les PVC tentent d'envoyer dépasse également le montant total de la largeur de bande disponible.
Résultat, la largeur de bande totale disponible (2 Mbps) est divisée proportionnellement au nombre de PVC:
2048 est la largeur de bande totale disponible et 512 kbps la vitesse la moins élevée. Ainsi, PVC 1 obtient 4/8th (1024 kbps) de la largeur de bande totale disponible, PVC 2 obtient 2/8ème (512 kbps), PVC 3 et 4 obtiennent chacun 1/8ème (256 kbps).

Scénario:

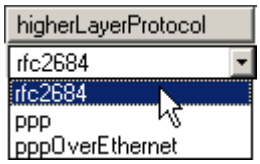
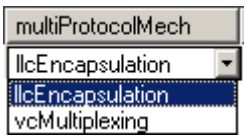
	PCR configuré	**Quantité de données envoyées**	**Largeur de bande assignée**
PVC 1	2048 kbps	2048 kbps	896 kbps
PVC 2	2048 kbps	2048 kbps	896 kbps
PVC 3	512 kbps	2048 kbps	192 kbps
PVC 4	1024 kbps	64 kbps	64 kbps

⇒Dans ce cas, les PCR des PVC sont surdimensionnés (c'est-à-dire que le total des PCR dépasse la largeur de bande de la connexion physique au réseau ATM). De plus, le montant total de données que les PVC tentent d'envoyer dépasse également le montant total de la largeur de bande disponible. Toutefois, un PVC (PVC 4) n'utilise pas la largeur de bande spécifiée dans son PCR.
Résultat, la largeur de bande totale disponible (2 Mbps) est divisée proportionnellement au nombre de PVC: La largeur de bande “de réserve” que le PVC 4 n'utilise pas est également divisée proportionnellement au trois PVC qui peuvent utiliser cette largeur de bande supplémentaire (PVC 1, 2 et 3).

MU-6.2.8 Configuration Ethernet/IP ponté/acheminé sur ATM (RFC 2684)

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour une introduction à Ethernet/IP ponté/acheminé sur ATM.

Pour configurer Ethernet/IP ponté/acheminé (multi-protocole) sur ATM sur un ATM PVC, procédez de la manière suivante:

Etape	Action
1	Dans pvcTable, sélectionnez la structure atm.
2	Dans la structure atm, réglez l'élément higherLayerProtocol sur rfc2684. En sélectionnant cette valeur, vous indiquez que différents types d'unités de données de protocole (PDU) peuvent être présents dans le trafic sur cette interface. 
3	Dans la structure atm, réglez l'élément multiProtocolMech sur le mécanisme d'encapsulation souhaité. En sélectionnant l'une de ces deux valeurs , vous indiquer comment les différents types d'unités de données de protocole (PDU) doivent être encapsulés dans ATM AAL type 5.  Dans le cas d'un … • llcEncapuslation, tous les types PDU différents sont transportés par un seul PVC. Dans ce cas, les différents types PDU peuvent être distingués les uns des autres par les informations contenues dans l'en-tête Logical Link Control (LLC). • vcMultiplexing, chaque type de PDU est transporté par un PVC distinct. Dans ce cas, vous devez configurer autant de PVC qu'il y a de types PDU dans votre trafic. De plus, l'application distante doit savoir quel PVC transporte quel type de PDU.

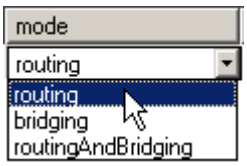
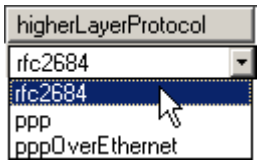
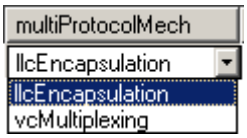
Reportez-vous à telindus1421Router/wanInterface/atm/pvcTable/atm page 36 pour une explication détaillée de la structure atm.

MU-6.2.9 Configuration d'IP classique IP (IPoA)

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour une introduction à IP sur ATM.

IP classique (RFC 1577) est l'une des encapsulations les plus fréquemment utilisées de IP sur ATM. La méthode d'encapsulation est la même que celle décrite dans RFC 2684 (anciennement RFC 1483). Le trafic IP est encapsulé sans en-tête Ethernet. L'ARP inversé est utilisé pour la résolution des adresses IP en canaux PVC.

Pour configurer Classical IP dans un ATM PVC, procédez de la façon suivante:

Etape	Action
1	Dans pvcTable, réglez l'élément mode sur routing. 
2	Dans pvcTable, sélectionnez la structure atm.
3	Dans la structure atm, réglez l'élément higherLayerProtocol sur rfc2684. 
4	Dans la structure atm, réglez l'élément multiProtocolMech sur le mécanisme d'encapsulation souhaité. llcEncapuslation ou vcMultiplexing. 

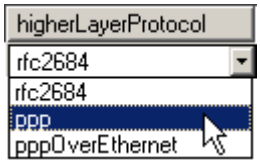
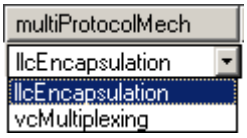
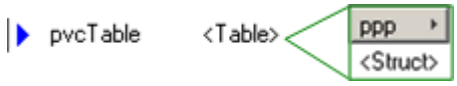
Reportez-vous à telindus1421Router/wanInterface/atm/pvcTable/atm page 36 pour une explication détaillée de la structure atm.

Notez que Inverse ARP est toujours utilisé. Par conséquent, il n'y a pas d'attribut spécifique pour activer ou désactiver InARP.

MU-6.2.10 Configuration PPP sur ATM (PPPoA)

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour une introduction à PPP sur ATM.

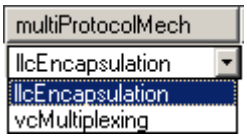
Pour configurer PPP sur ATM sur un ATM PVC, procédez de la façon suivante:

Etape	Action
1	Dans pvcTable, sélectionnez la structure atm.
2	Dans la structure atm, réglez l'élément higherLayerProtocol sur ppp. 
3	Dans la structure atm, réglez l'élément multiProtocolMech sur le mécanisme d'encapsulation souhaité. llcEncapuslation ou vcMultiplexing. 
4	Dans pvcTable, sélectionnez la structure ppp. 
5	Dans la structure ppp, configurez les éléments PPP (contrôle de liaison, authentification, etc.). Reportez-vous au… • MU-6.4 - Configuration d'encapsulation PPP page 121 pour de plus amples informations surla configuration PPP. • Reportez-vous à MR-1.5.3 - PPP configuration attributes page 52 pour une description détaillée des éléments de la structure ppp.

MU-6.2.11 Configuration PPP sur Ethernet (PPPoE)

Reportez-vous à MU-6.2.1 - Introduction à ATM page 85 pour une introduction à PPP sur Ethernet.

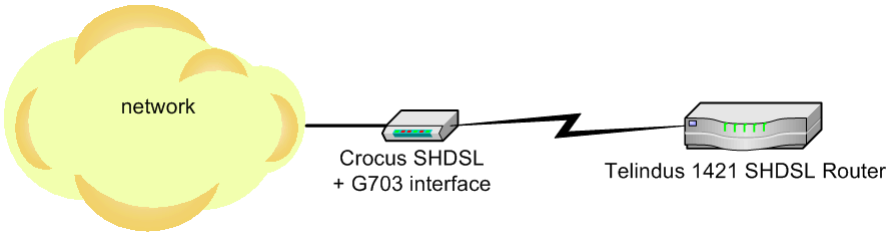
Pour configurer PPP sur Ethernet dans un ATM PVC, procédez de la façon suivante:

Etape	Action
1	Dans pvcTable, sélectionnez la structure atm.
2	Dans la structure atm, réglez l'élément higherLayerProtocol sur pppOverEthernet.
3	Dans la structure atm, réglez l'élément multiProtocolMech sur llcEncapsulation. 

MU-6.2.12 Configuration ATM sur une interface G703

L'interface du routeur Crocus 10M utilisée en combinaison avec une quelconque autre unité ne supporte pas l'interface ATM sur a G703. Seul le routeur Telindus 1421 SHDSL et les routeurs Telindus 1031/ 1032 peuvent fonctionner comme spécifié dans la norme G.804. Cela est dû au fait que l'interface du routeur Crocus 10M ne sait pas que les cellules ATM sont alignées par octets dans la trame G704.

ATM sur G703 en cas de Routeur Telindus 1421 SHDSL:



Sur le routeur, configurez les éléments suivants:

- réglez l'attribut telindus1421Router/wanInterface/line/timingMode sur plesiochronous.

Sur le Crocus SHDSL, configurez les éléments suivants:

- réglez l'attribut line/timingMode sur plesiochronous.
- utiilisez l'attribut g703/timeSlots pour sélectionner les intervalles de temps 1 à 15 et 17 à 31.

MU-6.3 Configuration d'encapsulation de Frame Relay

Cette section présente le protocole d'encapsulation Frame Relay et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-6.3.1 - Introduction au Frame Relay page 106
- MU-6.3.2 - Configuration de DLCI de Frame Relay page 111
- MU-6.3.3 - Obtention automatique d'adresses IP dans Frame Relay page 113
- MU-6.3.4 - Configuration d'adresses IP dans Frame Relay page 114
- MU-6.3.5 - Configuration LMI page 117
- MU-6.3.6 - Configuration CIR et EIR page 118
- MU-6.3.7 - Activation de la fragmentation Frame Relay page 120

MU-6.3.1 Introduction au Frame Relay

Qu'est-ce que le Frame Relay?

Le Frame Relay (relais de trame) est un protocole d'interconnexion qui travaille aux deux derniers niveaux inférieurs du modèle de référence OSI: les couches physique et de liaison de données. C'est un exemple de technologie de commutation par paquets, qui active les stations terminales pour partager les ressources du réseau de manière dynamique.

Les unités Frame Relay se répartissent dans les deux catégories générales suivantes:

- le matériel de terminal de données (DTEs), qui comprend les terminaux, les ordinateurs personnels, les routeurs et les ponts.
- le matériel de circuit de données (DCE), qui transmet les données par le biais du réseau. Il s'agit souvent d'un matériel dont le détenteur est le propriétaire.

Qu'est-ce qu'un DLCI?

Les réseaux Frame Relay transfèrent les données en utilisant l'un des types de connexion suivants:

- Les circuits virtuels commutés (SVC), qui sont des connexions temporaires créées pour chaque transfert de données et qui s'achèvent lorsque le transfert est terminé (ce type de connexion n'est pas très utilisé).
- Les circuits virtuels permanents (PVC), qui sont des connexions permanentes.

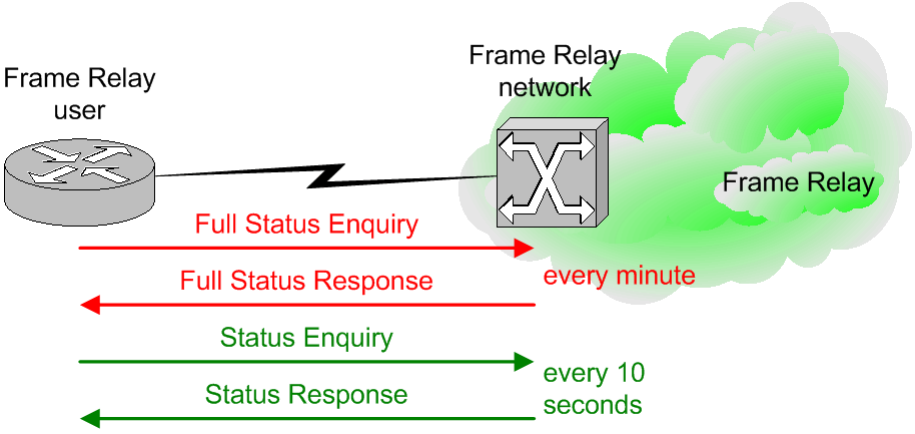
Le Routeur Telindus 1421 SHDSL utilise les circuits virtuels permanents. Le DLCI (Data Link Connection Identifier) est une valeur affectée à chaque circuit virtuel et à chaque point de connexion d'unité DTE dans le WAN à Frame Relay. Deux connexions différentes peuvent se voir affecter la valeur valeur dans le même WAN à Frame Relay, une de chaque côté de la connexion virtuelle.

Qu'est-ce que LMI?

Il existe un ensemble d'améliorations Frame Relay, appelé Local Management Interface (LMI). Le LMI offre un grand nombre de fonctions (appelées extensions) permettant de gérer des réseaux complexes, notamment:

- l'adressage global,
- les messages d'état de circuit virtuel,
- la multidiffusion.

LMI apporte un mécanisme d'état qui fournit un rapport d'état permanent en ligne sur les DLCI. Ces rapports d'état sont échangés entre l'unité d'accès Frame Relay (ou le DTE Frame Relay ou l'utilisateur) et le nœud Frame Relay (ou le DCE Frame Relay DCE ou le réseau).



A intervalles réguliers (typiquement chaque minute), l'utilisateur Frame Relay (p. ex. un routeur) envoie des messages de demande d'état complet au réseau de Frame Relay (p. ex. une commutation Frame Relay). A son tour, le réseau Frame Relay envoie une réponse d'état complète à l'utilisateur. Dans cette réponse, le réseau Frame Relay indique quel DLCI sont configurés et lesquels sont actifs ou hors service. Jusqu'à ce que le premier échange de demande d'état complet intervienne, l'utilisateur Frame Relay ne sait pas quels DLCI sont actifs et aucun transfert de données ne peut donc se faire.

A intervalles plus courts (typiquement, toutes mles 10 secondes), l'utilisateur Frame Relay envoie des messages de demande d'état au réseau Frame Relay. A son tour, le réseau Frame Relay envoie une réponse d'état complète à l'utilisateur. Dans cette réponse, le réseau Frame Relay indique uniquement quels DLCI sont actifs et hors service.

Il existe plusieurs versions de LMI: LMI rev.1, ANSI T1.617 Annexe D, Q.933 Annexe A, etc., assure l'interopérabilité avec votre réseau lorsque celui-ci se compose de matériels provenant de différents fabricants. La même version du protocole LMI doit se trouver à chaque extrémité de la liaison Frame Relay.

Que sont CIR et BC?

- CIR = BC / TC
- Le Committed Information Rate (CIR) est la quantité spécifiée de largeur de bande garantie (mesurée en bits par seconde) sur un service Frame Relay. Typiquement, à l'achat d'un service Frame Relay, le client peut spécifier le niveau de CIR qu'il souhaite. Le fournisseur de réseau Frame Relay garantit que le trafic ne dépassant pas ce niveau sera assuré.
- Le Committed Burst (BC) est la quantité maximale de données (en bits) que le réseau s'engage à transférer, dans des conditions normales, durant un intervalle de temps TC.

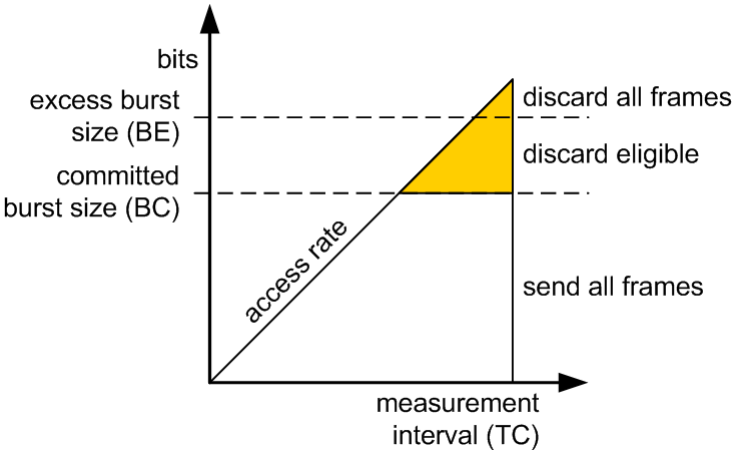
Que sont EIR et BE?

- EIR = BE / TC
- Le Excess Information Rate (EIR) est la quantité spécifiée de largeur de bande non garantie (mesurée en bits par seconde) sur un service Frame Relay. C'est le trafic excédentaire du CIR. Ce trafic peut également être assuré, mais rien ne le garantit.
- Le Excess Burst (BE) est la quantité maximum de données non engagées (en bits) en excédent de BC qu'un réseau Frame Relay peut tenter de fournir durant un intervalle de temps TC. Généralement, les données BE sont fournies avec une probabilité plus faible que BC, et le réseau les traite comme pouvant être rejetées.

Qu'est-ce que TC?

L'intervalle de mesure (TC) est la durée pendant laquelle les tailles de débit et d'impulsions sont mesurées. En général, la durée d'un TC est proportionnelle à la tendance aux impulsions d'un trafic.

La figure qui suit montre la relation entre BC, BE et TC:



Qu'est-ce que DE?

Lorsque le CIR est dépassé, toutes les trames qui suivent sont repérées comme pouvant être rejetées en réglant le bit DE dans l'en-tête du Frame Relay. Cela se fait sur le commutateur Frame Relay local. Si un encombrement se produit dans le réseau Frame Relay, les paquets marqués DE sont les premiers rejetés. Lorsqu'il détecte un encombrement, le commutateur Frame Relay renvoie un message Backward Explicit Congestion Notifier (BECN) à la source. Si la source (p. ex. le routeur) a une mémoire suffisante pour traiter ce message, il peut le retourner au CIR.

Qu'est-ce que BECN?

Backward Explicit Congestion Notification (BECN) est un bit défini par un réseau Frame Relay dans les trames se déplaçant dans le sens opposé à celui des trames rencontrant un encombrement. Les DTE recevant les trames avec le bit BECN réglé ainsi peuvent demander que des protocoles de niveau supérieur prennent les mesures de contrôle de flux adéquates.

Qu'est-ce que FECN?

Forward Explicit Congestion Notification (FECN) est un bitréglé par un réseau Frame Relay pour informer les DTE recevant la trame qu'un encombrement a été rencontré dans le trajet entre la source et la destination. Les DTE recevant les trames avec le bit FECN réglé ainsi peuvent demander que des protocoles de niveau supérieur prennent les mesures de contrôle de flux adéquates.

Qu'est-ce que la fragmentation de Frame Relay?

La fragmentation d'interface est utilisée pour permettre aux trames de données de partager en temps réel la même interface (physique). La fragmentation est strictement locale à l'interface et assure la temporisation adéquate et la variation de temporisation en fonction de la vitesse logique de l'interface (la vitesse logique d'une interface peut être plus lente que la vitesse de synchronisation physique si une interface physique canalisée est utilisée). La fragmentation étant locale à l'interface, le réseau peut profiter des vitesses de réseau plus importantes pour transporter les trames complètes, ce qui est plus efficace que de transporter un grand nombre de fragments plus petits.

La fragmentation d'interface est également utile en cas de non correspondance de vitesse entre les deux DTE aux extrémités d'un VC. Elle permet également au réseau de servir de proxy pour un DTE qui n'utilise pas la fragmentation de bout en bout. Reportez-vous à Qu'est-ce que la fragmentation de Frame Relay de bout en bout? page 109.

La fragmentation d'interface n'est *pas* transparene pour le réseau Frame Relay. C'est-à-dire que les commutateurs Frame Relay du réseau doivent “comprendre” la fragmentation.

La fragmentation d'interface est assurée sur une base interfac par interface. Lorsque la fragmentation d'interface est utilisée sur une interface, toutes les trames de tous les DLCI (y compris DLCI 0) sont précédées de l'en-tête de fragmentation.

Reportez-vous à FRF.12 pour de plus amples informations sur la fragmentation Frame Relay.

Qu'est-ce que la fragmentation de Frame Relay de bout en bout?

La fragmentation de bout en bout est utilisée sur les DLCI uniquement. Elle est utile lorsque des DTE de Frame Relay pairs souhaitent échanger du trafic en temps réel et non réel en utilisant une interface plus lente, mais qu'aucune des deux interfaces ne supporte la fragmentation d'interface Frame Relay. Reportez-vous à Qu'est-ce que la fragmentation de Frame Relay? page 109.

La fragmentation Frame Relay de bout en bout est transparent pour le réseau, c'est-à-dire que les commutateurs de Frame Relay du réseau n'ont pas à “connaître” la fragmentation.

DLCI 0 n'étant jamais transporté de bout en bout, il n'est jamais fragmenté en utilisant la fragmentation Frame Relay de bout en bout.

Reportez-vous à FRF.12 pour de plus amples informations sur la fragmentation Frame Relay.

Qu'est-ce que MLFR?

Multilink Frame Relay (MLFR) assure une émulation d'interface physique pour les unités Frame Relay. L'interface physique émulée se compose d'une ou de plusieurs liaisons physiques, appelées "faisceaux de liaisons", agrégées en un "faisceau" de largeur de bande unique. Ce service offre une fonction de multiplexage inversée basée sur les trames, parfois appelée "IMUX".

Le faisceau offre les mêmes services de conservation d'ordre qu'une couche physique aux trames envoyées sur une connexion de liaison de données. De plus, ce faisceau fournit un support à tous les services Frame Relay basés sur les normes UNI et NNI.

Reportez-vous à FRF.16 pour de plus amples informations sur le Frame Relay multiliaisons.

Qu'est-ce que le LIP?

Le Link Integrity Protocol (LIP) présente un ensemble de messages de contrôle permettant de s'assurer de l'intégrité du faisceau Frame Relay. Ces messages sont:

message LIP	Description
Add Link	Le message Add Link indique au terminal pair que le terminal local supporte le traitement le traitement de trame. Ce message comprend les informations requises pour vérifier l'apprtenance au faisceau et détecter les boucles en retour. Les deux extrémités d'un faisceau génèrent ce message lorsqu'un terminal de faisceau est prêt à devenir opérationnel.
Add Link Acknowledge	Le message Add Link Acknowledge notifie au terminal pair que le terminal local a reçu un message Add Link valable.
Add Link Reject	Le message Add Link Reject notifie au terminal pair que le terminal local a reçu un message Add Link non valable.
Hello	Le message Hello notifie au terminal pair que le terminal local reste actif. Les deux extrémités d'un faisceau génèrent régulièrement ce message.
Hello Acknowledge	Le message Hello Acknowledge notifie au terminal pair que le terminal local a reçu un message Hello valable.
Remove Link	Le message Remove Link notifie au pair que la fonction de gestion du terminal local supprime la liaison de ce faisceau.
Remove Link Acknowledge	Le message Hello Acknowledge notifie au terminal pair que le terminal local a reçu un message Hello valable.

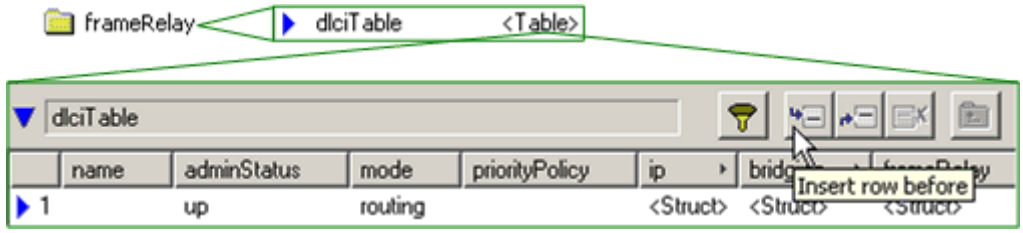
MU-6.3.2 Configuration de DLCI de Frame Relay

Reportez-vous à MU-6.3.1 - Introduction au Frame Relay page 106 pour la présentation.

Si le réseau Frame Relay supporte LMI, le Routeur Telindus 1421 SHDSL peut alors apprendre ses DLCI actives et inactives. Si le réseau Frame Relay supporte également le protocole InARP (Inverse Address Resolution Protocol), le Routeur Telindus 1421 SHDSL peut apprendre l'adresse IP du routeur correspondant pour chaque DLCI.

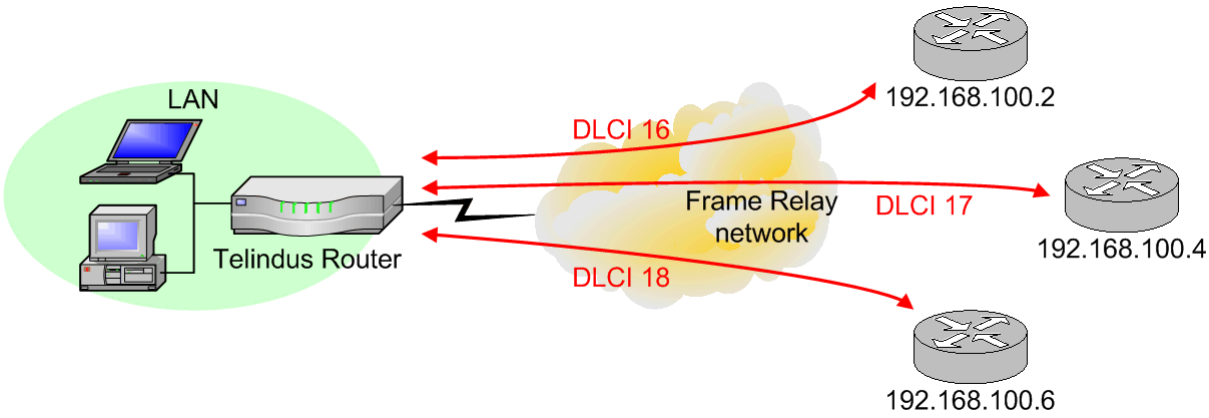
Si ni LMI ni InARP ne sont supportés par le réseau Frame Relay, vous pouvez configurer les DLCI vous-mêmes en utilisant dlciTable.

Pour configurer un DLCI Frame Relay, procédez de la manière suivante:

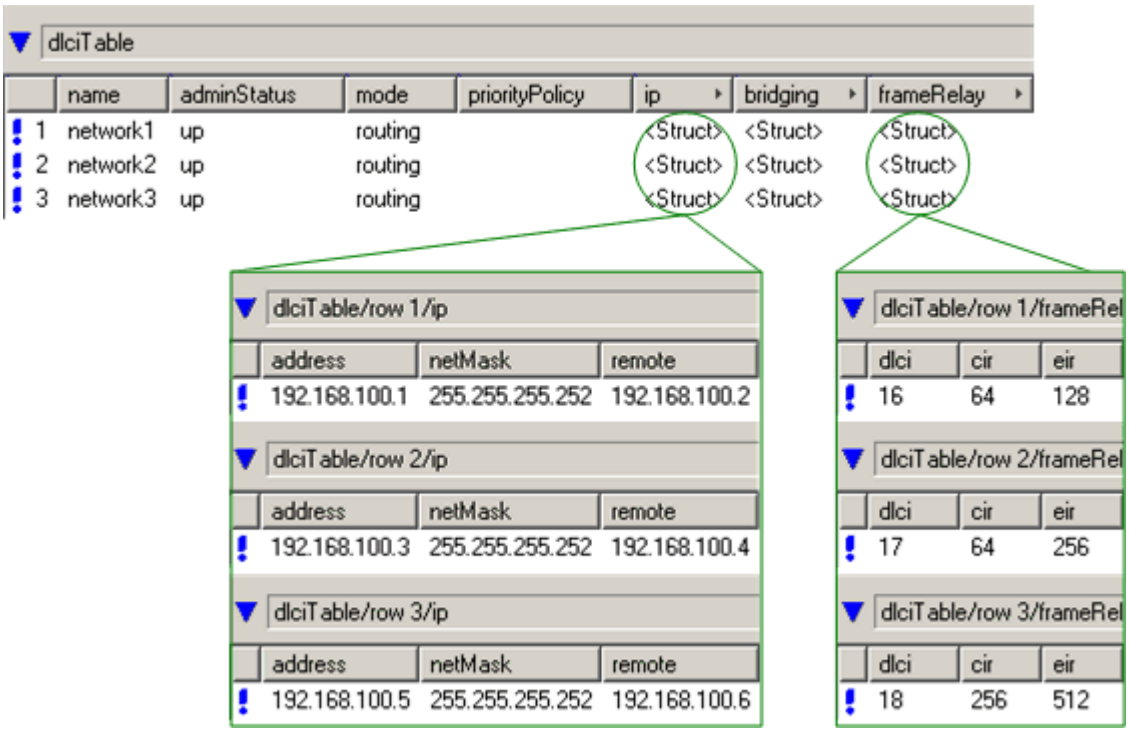
Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet frameRelay, sélectionnez l'attribut dlciTable et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour configurer les DLCI Frame Relay. Ajoutez une ligne au tableau dlciable pour chaque DLCI que vous souhaitez créer.
2	Configurez les éléments du DLCI que vous venez de créer. Ces éléments sont: • name. Utilisez cet élément pour assigner un nom administratif au DLCI Frame Relay. • adminStatus. Utilisez cet élément pour activer (up) ou désactiver (down) le DLCI. • mode. Utilisez cet élément pour déterminer si, pour le DLCI correspondant, les paquets sont traités par le processus d'acheminement, de pontage ou les deux. • priorityPolicy. Utilisez cet élément pour appliquer une politique de priorité au DLCI. Reportez-vous à MU-7.8.7 - Application d'une politique de priorité sur une interface page 215 pour de plus amples informations. • ip. Utilisez cet élément pour configurer les paramètres IP du DLCI. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour de plus amples informations. • bridging. Utilisez cet élément pour configurer les paramètres de pontage du DLCI si le DLCI est en mode de pontage (c'est-à-dire si l'élément mode est réglé sur bridging). Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 pour de plus amples informations. • frameRelay. Utilisez cet élément pour configurer les paramètres spécifiques du DLCI du Frame Relay. Reportez-vous à telindus1421Router/wanInterface/frameRelay/dlciTable/frameRelay page 45 pour de plus amples informations. Reportez-vous à telindus1421Router/wanInterface/frameRelay/dlciTable page 43 pour une description détaillée de dlciTable.

Exemple - configuration de DLCI de Frame Relay

La figure qui suit donne un exemple de segment Ethernet local connecté à trois réseaux différents par trois DLCI différents:



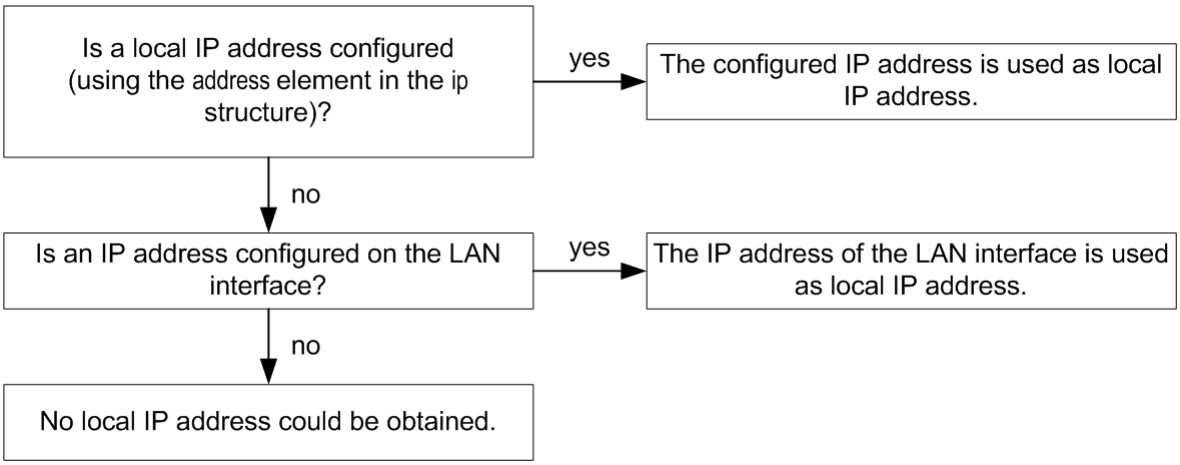
L'écran qui suit montre (en partie) la dlciTable de la configuration décrite dans la figure ci-dessus:



MU-6.3.3 Obtention automatique d'adresses IP dans Frame Relay

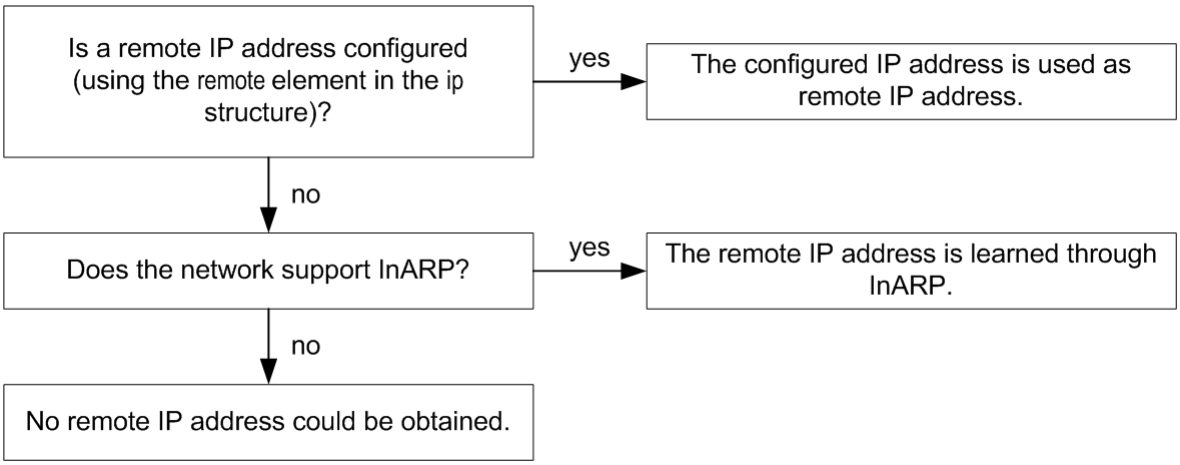
Obtention d'une adresse IP locale

Dans le cas de Frame Relay, le Routeur Telindus 1421 SHDSL ne supporte pas actuellement une procédure automatique d'apprentissage de l'adresse IP locale d'un DLCI de Frame Relay. Toutefois, si vous ne configurez pas l'adresse IP locale, l'adresse IP de l'interface LAN est utilisée.


Is a local IP address configured (using the address element in the ip structure)?
yes
The configured IP address is used as local IP address.
no
Is an IP address configured on the LAN interface?
yes
The IP address of the LAN interface is used as local IP address.
no
No local IP address could be obtained.

Obtention d'une adresse IP distante

Si le réseau Frame relay supporte le protocole InARP (Inverse Address Resolution Protocol), le Routeur Telindus 1421 SHDSL peut apprendre l'adresse IP distante d'un DLCI de Frame Relay.


Is a remote IP address configured (using the remote element in the ip structure)?
yes
The configured IP address is used as remote IP address.
no
Does the network support InARP?
yes
The remote IP address is learned through InARP.
no
No remote IP address could be obtained.

MU-6.3.4 Configuration d'adresses IP dans Frame Relay

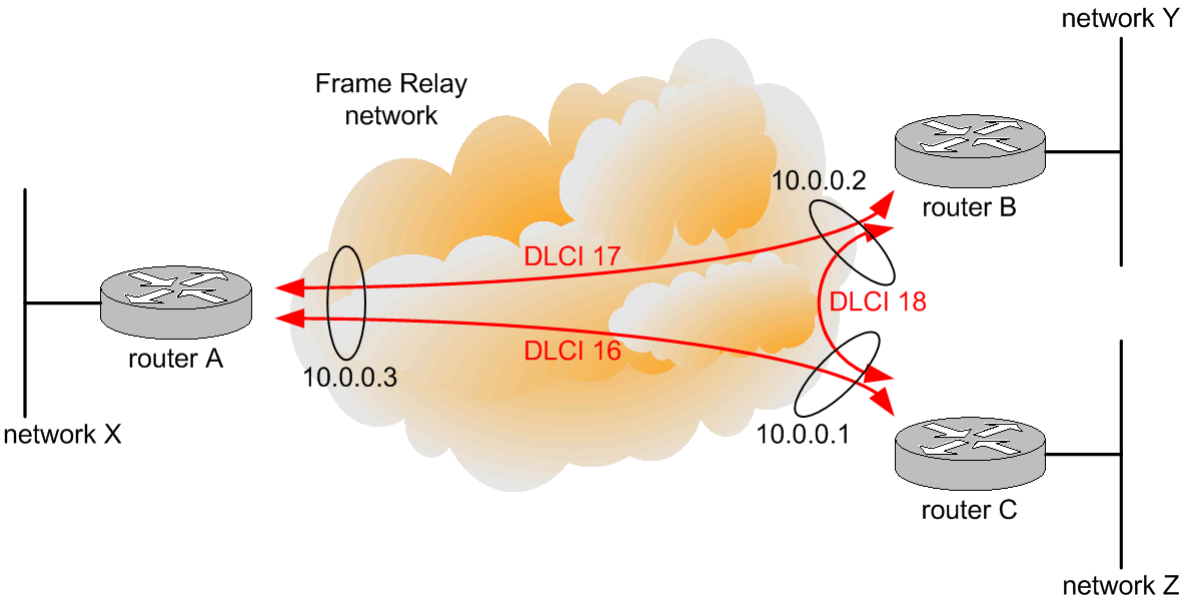
Lorsque vous utilisez l'encapsulation Frame Relay sur l'interface WAN, vous pouvez configurer les paramètres IP à deux niveaux:

En utilisant la structure ip dans le …	**Utilisez cet élément pour configurer les paramètres de l'IP de...**
frameRelay.	tous les DLCI pour lesquels … • dans dlciTable aucune adresse IP n'est définie pour ce DLCI spécifique, • et l'élément mode est réglé sur routing ou routingAndBridgning. En d'autres termes, utilisez cet attribut pour configurer globalement les paramètres IP des DLCI. Reportez-vous à Exemple – IP globale DLCI.
dlciTable.	un DLCI spécifique. Reportez-vous à Exemple – IP spécifique DLCI.

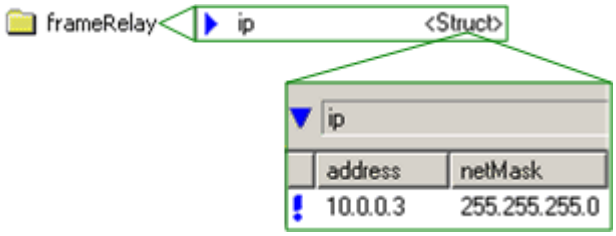
Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour une explication détaillée de la structure ip.

Exemple – IP globale DLCI

Supposons que vous ayez la configuration suivante:



Si vous considérez le routeur A, alors pour ce routeur …



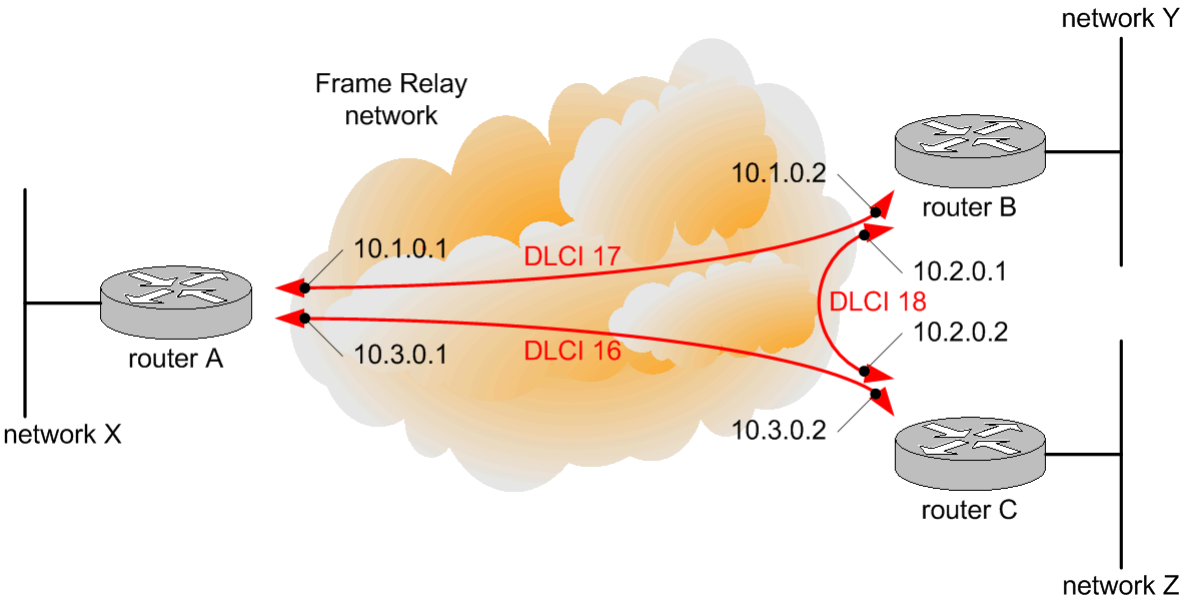
- deux DLCI sont configurés dans frameRelay/dlciTable, à savoir DLCI 16 et DLCI 17,
- aucune adresse IP n'est spécifiquement configurée pour ces DLCI,
- dans l'attribut frameRelay/ip, une adresse IP globale est configurée pour les DLCI, en l'occurrence 10.0.0.3.

Les caractéristiques d'une configuration avec adresse IP globale pour les DLCI sont les suivantes:

- Les diffusions sont copiées et envoyées à tous les DLCI (qui utilisent cette adresse IP globale). P. ex. appeler10.0.0.255 entraîne une réponse de 10.0.0.1, 10.0.0.2 et 10.0.0.3.
- Appeler 10.0.0.3 entraîne une réponse lorsque LMI est actif.
- Les trajets appris par un DLCI ne sont pas transmis aux autres DLCI. P. ex., un trajet appris par DLCI 16 n'est pas transmis au DLCI 17. Cela signifie qu'un horizon partagé est applicable.
- RIP uniquement les fonctions si le réseau est totalement entrelacé, c'est-à-dire si chaque routeur est directement connecté à ses voisins par un DLCI (comme dans l'exemple ci-dessus).

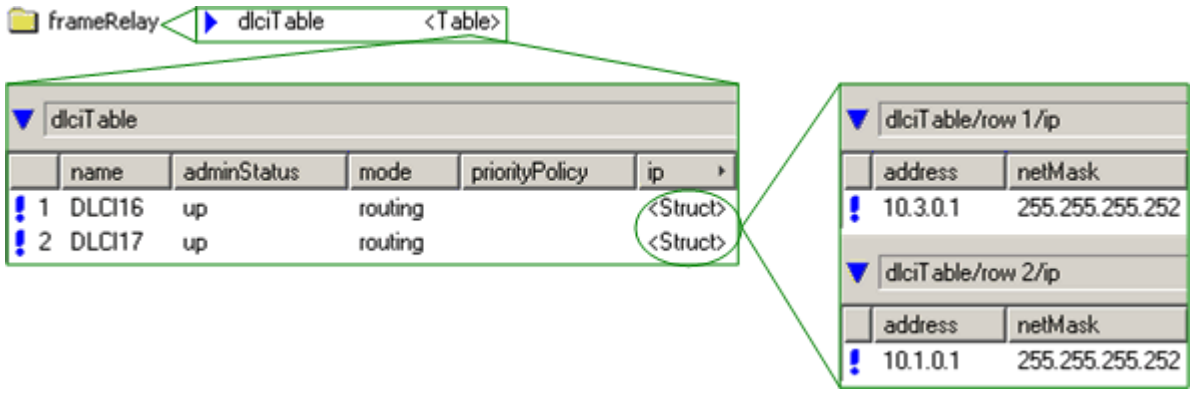
Exemple – IP spécifique DLCI

Supposons que vous ayez la configuration suivante:



Si vous considérez le routeur A, alors pour ce routeur …

- deux DLCI sont configurés dans frameRelay/dlciTable, à savoir DLCI 16 et DLCI 17,
- une adresse IP est spécifiquement configurée pour chaque DLCI dans l'attribut frameRelay/dlciTable/ip,
- aucune adresse IP globale n'est configurée pour les DLCI.



Les caractéristiques d'une configuration avec adresse IP spécifique pour les DLCI sont les suivantes:

- Chaque DLCI est une interface IP.
- Appeler 10.1.0.1 entraîne une réponse lorsque le DLCI est actif.
- Les trajets appris par un DLCI sont transmis aux autres DLCI. P. ex., un trajet appris par DLCI 16 est transmis au DLCI 17. Cela signifie qu'un horizon partagé n'est pas applicable.

MU-6.3.5 Configuration LMI

Reportez-vous à MU-6.3.1 - Introduction au Frame Relay page 106 pour une introduction au LMI.

Pour configurer LMI, procédez de la façon suivante:

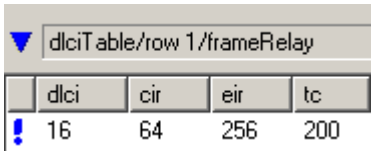
Etape	Action
1	Dans l'objet frameRelay, sélectionnez la structure lmi.
2	Les éléments les plus importants de la structure lmi sont: • mode. Utilisez cet élément pour régler le mode Frame Relay (user, network, auto ou nni). • type. Utilisez cet élément pour définir la variante LMI. Il existe plusieurs normes de protocole LMI, qui présentent de légères variations l'une par rapport à l'autre. Par conséquent, configurez le Routeur Telindus 1421 SHDSL en fonction de la norme utilisée par votre fournisseur de services. Reportez-vous à telindus1421Router/wanInterface/frameRelay/lmi page 47 pour une description complète de la structure lmi.

MU-6.3.6 Configuration CIR et EIR

Reportez-vous à MU-6.3.1 - Introduction au Frame Relay page 106 pour une introduction à CIR et EIR.

Comme nous l'avons vu plus haut, CIR est la vitesse de données à laquelle l'utilisateur souhaite passer sur le réseau Frame Relay sans grand problème. Notez que le CIR n'est pas lié à la vitesse binaire effective de la connexion physique. Un utilisateur peut avoir une connexion physique fonctionnant à 2 Mbps, mais un CIR sur cette connexion physique de seulement 64 kbps. Cela signifie que la vitesse moyenne de données de l'utilisateur est de 64 kbps, mais que les données peuvent parfois monter jusqu'à 2 Mbps (EIR).

Pour configurer CIR et EIR dans un DLCI Frame Relay, procédez de la façon suivante:

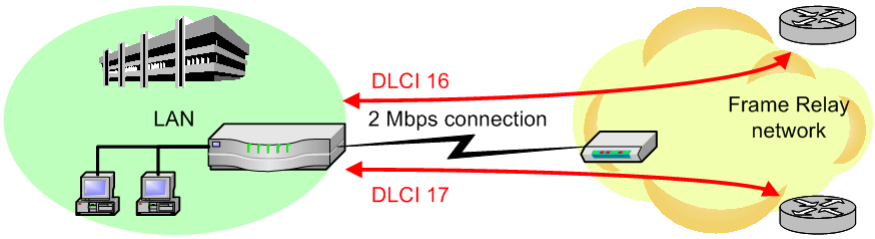
Etape	Action
1	Dans dlciTable, sélectionnez la structure frameRelay.
2	Dans la structure frameRelay, configurez les éléments suivants:  • cir. Utilisez cet élément pour régler le CIR du DLCI. Le cir est exprimé en bps. Entrez un multiple de 64000 bps comme valeur cir (p. ex. 2048000). La valeur maximale est la connexion physique au réseau Frame Relay. Si la valeur cir est réglée sur 0 (par défaut), cela signifie que toute la largeur de bande peut être utilisée (pas de contrôle de flux). • eir. Utilisez cet élément pour régler l'EIR du DLCI. The eir est exprimé en bps. Entrez un multiple de 64000 bps comme valeur eir (p. ex. 2048000). La valeur maximale est la connexion physique au réseau Frame Relay. Si la valeur eir est réglée sur 0 (par défaut), cela signifie qu'aucune impulsion supplémentaire n'est autorisée. Les impulsions de données qui sont autorisées sont la valeur CIR + la valeur EIR. Si vous souhaitez un CIR de 1 Mbps et souhaitez autoriser les impulsions jusqu'à 1,5 Mbps, réglez le CIR sur 1024000 bps et l'EIR sur 512000 bps.

Remarques importantes

- Veillez à ne pas surdimensionner le CIR (c'est-à-dire ne laissez pas le total des CIR des DLCI dépasser la largeur de bande de la connexion physique).
- Lorsque vous dépassez la largeur de bande totale de la connexion physique, le Routeur Telindus 1421 SHDSL met les données en mémoire tampon. Toutefois, si les mémoires tampons du Routeur Telindus 1421 SHDSL sont remplies, elles doivent rejeter les données en “surplus”.
- Pour obtenir un QoS optimal pour les liaisons qui contiennent des DLCI vocaux et de données, il est recommandé d'utiliser le CIR pour les DLCI vocaux et l'EIR pour les DLCI de données. Cela réduit la quantité de paquets de données mis en file d'attente dans une seule impulsion, réduisant ainsi la temporisation de transmission des paquets vocaux.

Exemples

Supposons que vous ayez une connexion physique de 2 Mbps vers le fournisseur de services Frame Relay et que vous définissiez 2 DLCI:



- Supposons que vous affectiez aux deux DLCI un CIR de 1 Mbps et un EIR de 0.

  ⇒Dans ce cas, vous avez pour chaque DLCI une largeur de bande garantie de 1 Mbps et aucune impulsion n'est admise.

- Supposons que vous affectiez aux deux DLCI un CIR de 512 Mbps et un EIR de 512.

  ⇒Dans ce cas, pour avez pour chaque DLCI une largeur de bande garantie de 512 kbps et vous autorisez des impulsions jusqu'à 1 Mbps. Cela signifie que si sur les deux DLCI, il se produit une impulsion jusqu'à 1 Mbps en même temps, la vitesse de la connexion physique (2 Mbps) n'est pas encore dépassée (et aucune donnée n'est rejetée). Si toutefois un encombrement se produit ailleurs dans le réseau, il est possible qu'une partie des données “excédentaires” soit rejetée (voir Qu'est-ce que DE? page 108).

- Supposons que vous affectiez aux deux DLCI un CIR de 1 Mbps et un EIR de 1.

  ⇒Dans ce cas, pour avez pour chaque DLCI une largeur de bande garantie de 1 Mbps et vous autorisez des impulsions jusqu'à 2 Mbps. Cela signifie que si sur les deux DLCI, il se produit une impulsion jusqu'à 2 Mbps en même temps, la vitesse de la connexion physique (2 Mbps) est dépassée (et certaines données sont rejetées). Dans ce cas, le principe qui s'applique est celui du premier venu – premier servi. Le DLCI sur lequel l'impulsion s'est produite en premier voit ses données passer dans le réseau Frame Relay. Si toutefois un encombrement se produit ailleurs dans le réseau, il est possible qu'une partie des données “excédentaires” soit rejetée.

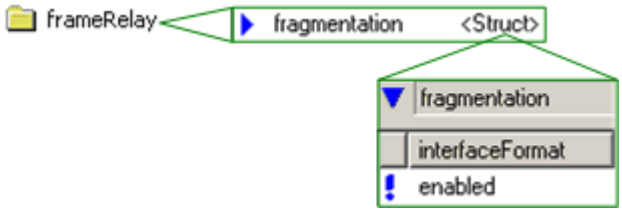
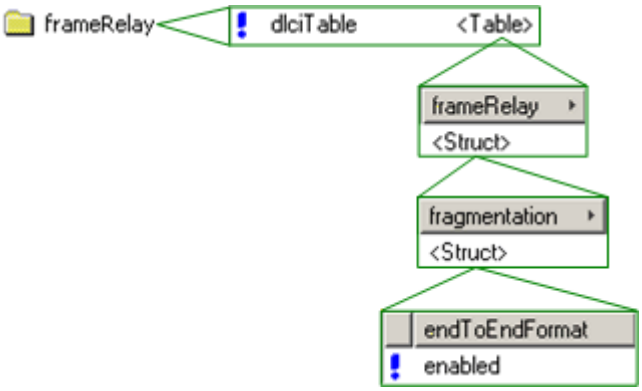
- Supposons que vous affectiez aux deux DLCI un CIR de 2 Mbps et un EIR de 0.

  ⇒Dans ce cas, vous avez surdimensionné votre CIR. Vous ne pouvez garantir 2 Mbps de largeur de bande pour les deux DLCI, du fait de la limite de largeur de bande de 2 Mbps de la connexion physique. Là encore, c'est le principe du premier venu – premier servi qui s'applique. Le DLCI qui a envoyé ses données en premier les voit passer sur le réseau Frame Relay.

MU-6.3.7 Activation de la fragmentation Frame Relay

Reportez-vous à MU-6.3.1 - Introduction au Frame Relay page 106 pour une introduction à la fragmentation Frame Relay.

Il existe différents cas de fragmentation. La table qui suit montre comment activer la fragmentation dans chacun de ces cas:

Cas	Comment activer la fragmentation?
1	**Fragmentation d'interface sur une interface** Pour activer la fragmentation Frame Relay au niveau de l'interface, pour une interface donnée, procédez de la façon suivante:  1. Sélectionnez l'objet frameRelay. 2. Sélectionnez la structure fragmentation. 3. Réglez l'élément interfaceFormat sur enabled.
2	**Fragmentation de bout en bout sur une interface** Pour activer la fragmentation Frame Relay de bout en bout, pour un DLCI donné sur une interface donnée, procédez de la façon suivante:  1. Sélectionnez l'objet frameRelay. 2. Sélectionnez dlciTable. 3. Sélectionnez la structure frameRelay. 4. Sélectionnez la structure fragmentation. 5. Réglez l'élément endToEndFormat sur enabled.

MU-6.4 Configuration d'encapsulation PPP

Cette section présente le protocole d'encapsulation PPP et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-6.4.1 - Introduction à PPP page 122
- MU-6.4.2 - Obtention automatique d'adresses IP dans PPP page 126
- MU-6.4.3 - Configuration d'adresses IP dans PPP page 128
- MU-6.4.4 - Imposition d'adresses IP sur le côté distant dans PPP page 129
- MU-6.4.5 - Configuration de la surveillance de liaison page 130
- MU-6.4.6 - Configuration PAP page 131
- MU-6.4.7 - Comment fonctionne le PAP? page 132
- MU-6.4.8 - Configuration CHAP page 134
- MU-6.4.9 - Comment fonctionne le CHAP? page 135
- MU-6.4.10 - Quels attributs de nom et de secret utiliser pour l'authentification PPP? page 137
- MU-6.4.11 - Configuration de PPP multiliaisons page 138
- MU-6.4.12 - Activation de la fragmentation PPP page 140
- MU-6.4.13 - Configuration de PPP multiclasses page 141

MU-6.4.1 Introduction à PPP

Qu'est-ce que PPP?

Le protocole point à point (PPP) est apparu à l'origine comme un protocole d'encapsulation pour le transport du trafic IP sur des liaisons point par point. PPP a également établi une norme d'affectation et de gestion des adresses IP, de l'encapsulation asynchrone et synchrone orienté bits, du multiplexage de protocole réseau, de la configuration de liaison, de test de qualité de liaison, de détection d'erreur, et de négociation optionnelle pour des capacités de mise en réseau supplémentaires.

Reportez-vous également à Qu'est-ce que PPPoA (RFC 2364)? page 90.

Que sont LCP, IPCP, BCP et CCP?

PPP est une méthode de transmission de datagrammes sur les liaisons série point par point, qui inclut les composantes suivantes:

- Une méthode d'encapsulation des datagrammes sur des liaisons série.
- Un protocole de contrôle de liaison extensible (LCP) qui permet d'établir, de configurer, de maintenir à jour et de terminer la connexion point par point.
- Une famille de protocoles de contrôle de réseau (NCP) permettant d'établir et de configurer différents protocoles de couche de réseau tels que IP Control Protocol (IPCP) et Bridge Control Protocol (BCP).
- Un protocole de contrôle de compression (CCP) permettant de configurer, d'activer et de désactiver les algorithmes de compression de données aux deux extrémités de la liaison point par point.

L'établissement de liaison PPP

PPP procède à un établissement de liaison en deux phases:

Phase	Description
1	Le Link Control Protocol (LCP) constitue la couche de liaison.
2	Le Network Control Protocol (NCP, c'est-à-dire IPCP ou BCP) constitue la couche réseau.

Qu'est-ce que le contrôle de liaison PPP?

PPP permet le contrôle de liaison pour vérifier si la liaison PPP est active ou non. Si le contrôle de liaison est activé, des paquets de demande en écho sont envoyés sur la liaison à intervalle régulier. Si aucune réponse n'est donnée à des demandes consécutives, la liaison PPP est déclarée inactive. Les données sont arrêtées jusqu'à ce que l'établissement de liaison PPP réussisse à nouveau.

Qu'est-ce que le PAP?

Le Password Authentication Protocol (PAP) est la forme d'authentification la plus basique (conforme à RF 1334). Elle fonctionne dans son principe de la même façon que la procédure de login. Le pair (le système authentificateur) s'authentifie lui-même en envoyant un nom d'utilisateur et un mot de passe à l'authentificateur. L'authentificateur compare alors ce nom d'utilisateur et ce mot de passe à sa base de données de renseignements. Si le mot de passe correspond, le pair est authentifié et la session peut être initialisée. L'authentification PAP peut se faire dans un seul sens ou dans les deux sens.

L'inconvénient du PAP est qu'il est vulnérable aux indiscrets qui peuvent tenter d'oobtenir le mot de passe en écoutant la ligne en série, et à des essais répétés et à des attaques d'erreur.

Qu'est-ce que le CHAP?

Le Challenge Handshake Authentication Protocol (CHAP) est plus sûr que le PAP.

Avec le CHAP, le serveur (l'authentificateur) envoie une chaîne de correspondance générée de manière aléatoire au client (le système d'authentification). Le client utilise cette chaîne, indique son mot de passe et son mot de passe en utilisant l'algorithme MD5. Le résultat est renvoyé au serveur. Le serveur effectue alors le même calcule et compare ce nom d'utilisateur et ce mot de passe avec sa base de données secrète. Si le mot de passe correspond, le pair est authentifié et la session peut être initialisée. L'authentification CHAP peut se faire dans un seul sens ou dans les deux sens.

Une autre caractéristique de CHAP est qu'il ne demande pas seulement au client de s'identifier lui-même en début de session, mais aussi de le faire à intervalles réguliers. Il le fait pour s'assurer que le client n'a pas été remplacé par un intrus (par exemple, à l'occasion d'une commutation de ligne).

Qu'est-ce que le MS-CHAP?

Le Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) est la version Microsoft du CHAP et constitue une extension de RFC 1994. Comme la version standard du CHAP, MS-CHAP est utilisé à des fins d'authentification PPP. Dans ce cas, l'authentification se produit entre un PC utilisant Microsoft et un routeur ou un serveur d'accès faisant office de serveur d'accès au réseau (NAS).

Les différences entre le CHAP standard et MS-CHAP sont les suivantes:

- MS-CHAP est activé en négociant l'algorithme CHAP 0x80 dans LCP option 3, protocole d'authentification.
- Le paquet de réponse MS-CHAP est un format conçu pour être compatible avec Microsoft Windows. Ce format n'eexige pas de l'authentificateur qu'il mémorise un mot de passe en clair ou encrypté.
- MS-CHAP est un mécanisme de nouvelle tentative d'authentification commandée par l'authentificateur.
- MS-CHAP est un mécanisme de changement de mot de passe commandé par l'authentificateur.
- MS-CHAP définit un ensemble de codes de "motif d'échec" qui est renvoyé dans le champ de message d'erreur.

Qu'est-ce que le MS-CHAPv2?

MS-CHAP version 2 offre une sécurité plus importante pour des connexions d'accès distantes et résoud également certains des problèmes de MS-CHAP version 1:

Problème MS-CHAP version 1	Solution MS-CHAP version 2
Le codage de la réponse du gestionnaire LAN utilisée pour la compatibilité matérielle avec d'anciens clients d'accès distants présente des défauts de cryptographie.	MS-CHAP v2 ne permet plus les réponses codées du gestionnaire LAN.
Le codage des modifications du mot de passe par le gestionnaire LAN présente des défauts de cryptographie.	MS-CHAP v2 ne permet plus les changements de mot de passe codés du gestionnaire LAN.
Seule uune authentification dans un sens est possible. Le client à accès distant ne peut pas vérifier si la numérotation se fait dans le serveur d'accès à distance de son organisation ou dans un serveur d'accès à distance d'usurpation d'identité.	MS-CHAP v2 permet une authentification dans les deux sens, appelée également authentification mutuelle. Le client à accès à distance reçoit la vérification que le serveur d'accès à distance dans lequel il numérote a accès au mot de passe de l'utilisateur.
Avec un cryptage par 40 bits, le code cryptographique est basé sur le mot de passe de l'utilisateur. Chaque fois que l'utilisateur se connecte avec le même mot de passe, le même code cryptographique est généré.	Avec MS-CHAP v2, le code cryptographique est toujours basé sur le mot de passe de l'utilisateur et sur une chaîne de contrôle arbitraire. Chaque fois que l'utilisateur se connecte avec le même mot de passe, un code cryptographique différent est généré.
Un code cryptographique unique est utilisé pour les données envoyées dans les deux sens de la connexion.	Avec MS-CHAP v2, des codes cryptographiques distincts sont générés pour les données transmises et reçues.

Qu'est-ce que le MLPPP?

Multilink PPP (MLPPP) est une méthode de séparation, de recombinaison et de séquençage des datagrammes sur des liaisons de données logiques multiples.

Malgré touts ses avantages, le PPP présente un inconvénient lorsqu'il s'agit de déploiement de réseau: il est conçu pour ne gérer qu'une seule liaison physique à la fois. Le MLPPP permet de surmonter cette limitation. Le MLPPP est un protocole de liaison de données de niveau supérieur, qui repose entre le PPP et la couche de protocole de réseau. Il traite une ou plusieurs liaisons PPP, chacune représentant soit une connexion WAN physique distincte, soit un canal dans un service commuté multicanaux. La capacité du MLPPP à combiner plusieurs liaisons de moindre vitesse en un seul trajet de données à plus grande vitesse est souvent appelée multiplexage indépendant du WAN ou multiplexage inverse basé sur les paquets.

Le MLPPP négocie les options de configuration de la même manière qu'un PPP conventionnel. Toutefois, lors du processus de négociation, un routeur ou une unité d'accès indique à l'autre unité de commande qu'il souhaite combiner plusieurs connexions et les traiter comme un seul conduit physique. Il le fait en envoyant un message d'option multiliaisons dans le cadre de sa négociation d'option LCP initiale.

Une fois la session multiliaisons ouverte, le MLPPP côté émetteur reçoit les unités de données du protocole réseau (PDU) en provenance des protocoles ou des applications de couche supérieure. Il fragmente alors ces PDU en paquets plus petits, ajoute un en-tête MLPPP à chaque fragment et les envoie par le biais des liaisons PPP disponibles. Côte réception, le logiciel MLPPP prend les paquets fragmentés dans les différentes liaisons, les remet dans l'ordre correct en fonction de leurs en-tête MLPPP et les reconvertit en PDU de couche réseau d'origine.

Qu'est-ce que la fragmentation PPP?

Avec le MLPPP, vous pouvez activer la fragmentation de paquets. Lorsque la fragmentation de paquets n'est pas activée, les paquets sont envoyés en entier sur les canaux. Lorsque la fragmentation de paquets est activée, les grands paquets sont divisés en fragments plus petits et répartis sur l'ensemble des canaux utilisés. Envoyer les paquets de cette manière réduit les temps de transit. Le récepteur collecte les fragments, les réassemble, et les remet dans l'ordre prévu à l'origine.

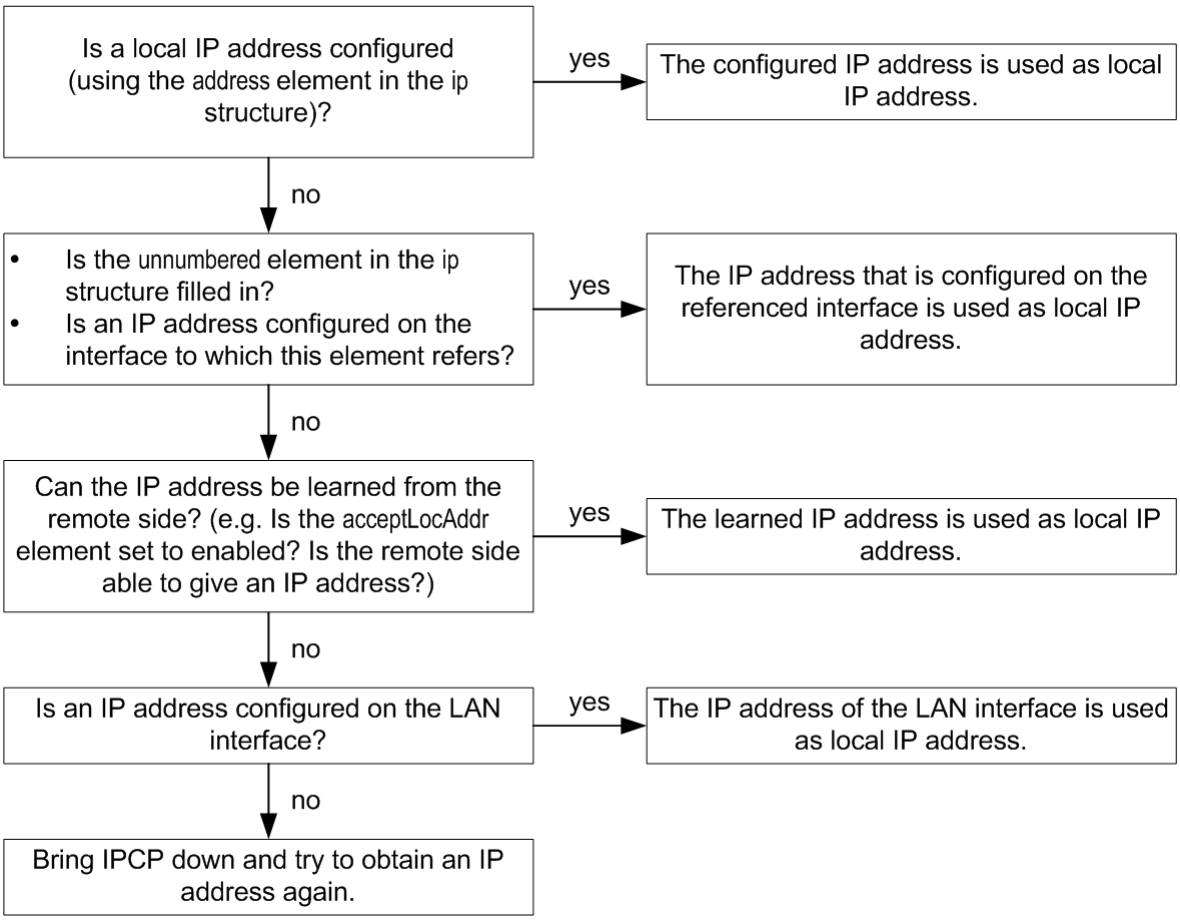
Qu'est-ce que le PPP multiclasses?

Le PPP multiclasses récupère certains bits inutilisés dans l'en-tête multiliaisons PPP pour permettre des flux distincts dans une seule session PPP. Cela permet de disposer de fonctions de type Frame Relay à l'intérieur de cette session PPP. Cela facilite également le QoS sur une seule liaison PPP. Tioutefois, le nombre de sessions possible est faible comparé au Frame Relay.

MU-6.4.2 Obtention automatique d'adresses IP dans PPP

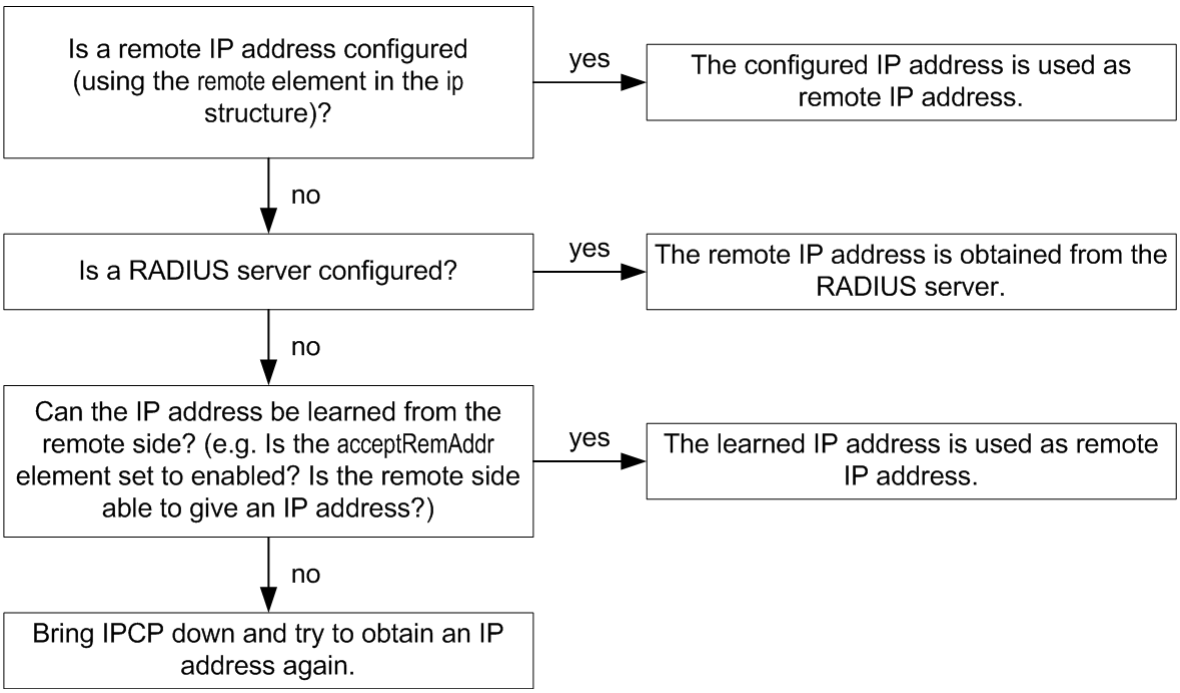
Obtention d'une adresse IP locale

Dans le cas de PPP, le Routeur Telindus 1421 SHDSL peut apprendre l'adresse IP locale d'une liaison PPP.


Is a local IP address configured (using the address element in the ip structure)?
yes
The configured IP address is used as local IP address.
no
• Is the unnumbered element in the ip structure filled in?
• Is an IP address configured on the interface to which this element refers?
yes
The IP address that is configured on the referenced interface is used as local IP address.
no
Can the IP address be learned from the remote side? (e.g. Is the acceptLocAddr element set to enabled? Is the remote side able to give an IP address?)
yes
The learned IP address is used as local IP address.
no
Is an IP address configured on the LAN interface?
yes
The IP address of the LAN interface is used as local IP address.
no
Bring IPCP down and try to obtain an IP address again.

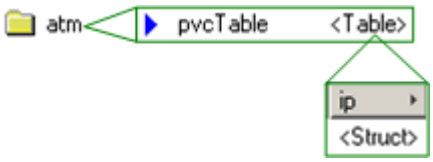
Obtention d'une adresse IP distante

Dans le cas de PPP, le Routeur Telindus 1421 SHDSL peut apprendre l'adresse IP distante d'une liaison PPP.


Is a remote IP address configured (using the remote element in the ip structure)?
yes
The configured IP address is used as remote IP address.
no
Is a RADIUS server configured?
yes
The remote IP address is obtained from the RADIUS server.
no
Can the IP address be learned from the remote side? (e.g. Is the acceptRemAddr element set to enabled? Is the remote side able to give an IP address?)
yes
The learned IP address is used as remote IP address.
no
Bring IPCP down and try to obtain an IP address again.

MU-6.4.3 Configuration d'adresses IP dans PPP

Pour configurer des adresses IP dans une liaison PPP(oA), procédez de la façon suivante:

Etape	Action
1	Si vous configurez une liaison PPP, vous devez configurer les paramètres liés à l'IP en utilisant la structureip dans l'objet ppp. Si vous configurez une liaison PPPoA (voir MU-6.2.10 - Configuration PPP sur ATM (PPPoA) page 102), vous configurez les adresses IP au niveau ATM PVC. Dans ce cas, vous devez donc configurer les paramètres liés à l'IP dans la structure ip de pvcTable. **Liaison PPP** Dans l'objet ppp, sélectionnez la structure ip. **Liaison PPPoA** Dans l'objet atm, sélectionnez pvcTable puis sélectionnez la structureip. 
2	Dans la structure ip, configurez les éléments suivants: • address. Utilisez cet élément pour affecter une adresse IP à l'extrémité locale de la liaison PPP(oA). • netMask. Utilisez cet élément pour affecter un masque de sous-écran IP à l'extrémité locale de la liaison PPP(oA). • remote. Utilisez cet élément pour affecter une adresse IP à l'extrémité distante de la liaison PPP(oA). • unnumbered. Si vous ne configurez pas explicitement une adresse IP locale pour une liaison PPP(oA), vous pouvez utiliser cet élément pour "emprunter" l'adresse IP d'une autre interface pour laquelle une adresse IP est déjà configurée. • acceptLocAddr. Utilisez cet élément pour déterminer si vous acceptez ou refusez l'adresse IP locale imposée par l'extrémité distante. • acceptRemAddr. Utilisez cet élément pour déterminer si vous acceptez ou refusez l'adresse IP distante imposée par l'extrémité distante. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour une explication détaillée de la structure ip.

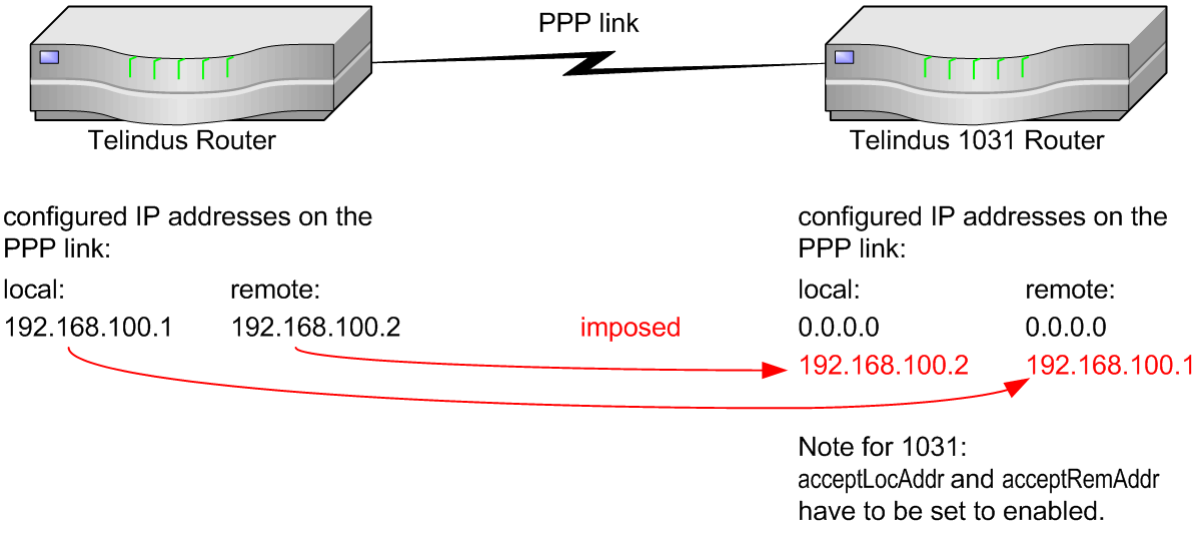
MU-6.4.4 Imposition d'adresses IP sur le côté distant dans PPP

Comme nous pouvons le voir dans MU-6.4.2 - Obtention automatique d'adresses IP dans PPP page 126, sdans le cas de PPP, le Routeur Telindus 1421 SHDSL peut apprendre les adresses IP depuis l'extrémité distante. De plus, dans le cas du PPP, le Routeur Telindus 1421 SHDSL lui-même peutimposer des adresses IP à l'unité distante.

Pour imposer des adresses IP à l'unité distante, procédez de la façon suivante:

Etape	Action
1	Sur le Routeur Telindus 1421 SHDSL, configurez une adresse IP locale et distante sur la liaison PPP. Reportez-vous à MU-6.4.3 - Configuration d'adresses IP dans PPP page 128.
2	Sur l'unité distante (p. ex. un routeur Telindus 1031), ne configurez ni adresse locale ni adresse distante sur la liaison PPP. ⇒Lorsque l'établissement de liaison PPP atteint le stade IPCP, le routeur Telindus 1031 déclare au Routeur Telindus 1421 SHDSL qu'il n'a pas d'adresses IP sur sa liaison PPP. Le Routeur Telindus 1421 SHDSL à son tour impose l'adresse IP locale et distante de la liaison PPP sur le routeur Telindus 1031. ⇒De plus, le routeur Telindus 1031 ajoute un trajet vers le Routeur Telindus 1421 SHDSL. Reportez-vous à l'explication de l'élément gatewayPreference page 57. Notez que les attributs de configuration IP acceptLocAddr et acceptRemAddr sur le routeur Telindus 1031 doivent être activés. Sinon, le routeur Telindus 1031 n'accepte pas les adresses IP imposées par le Routeur Telindus 1421 SHDSL.

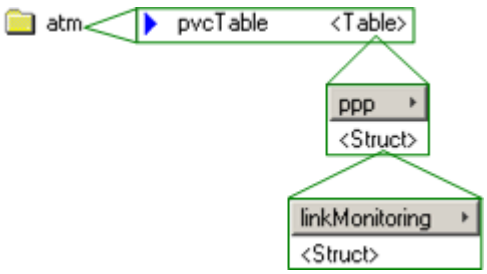
Exemple – imposition d'adresses IP sur l'unité distante dans PPP



MU-6.4.5 Configuration de la surveillance de liaison

Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction à la surveillance de liaison.

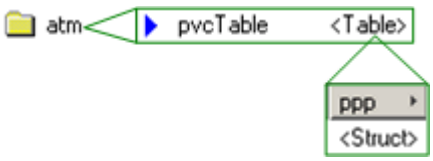
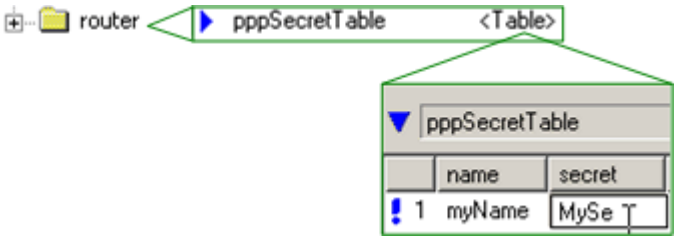
Pour configurer la surveillance de liaison sur une liaison PPP(oA), procédez de la façon suivante:

Etape	Action
1	**Liaison PPP** Dans l'objet ppp, sélectionnez la structure linkMonitoring. **Liaison PPPoA** Dans l'objet atm, sélectionnez pvcTable, puis sélectionnez la structure ppp et, enfin, la structure linkMonitoring. 
2	La structure linkMonitoring contient les éléments suivants: • operation. Utilisez cet attribut pour activer ou désactiver la surveillance de liaison. • interval. Utilisez cet élément pour définir l'intervalle de temps entre deux demandes consécutives. • replyTimeOut. Utilisez cet élément pour déterminer la durée pendant laquelle le Routeur Telindus 1421 SHDSL attend une réponse à sa demande d'écho. • failsPermitted. Utilisez cet élément pour définir le nombre de demandes d'écho pouvant échouer avant que le Routeur Telindus 1421 SHDSL ne déclare la liaison PPP inactive. Reportez-vous à telindus1421Router/wanInterface/ppp/linkMonitoring page 55 pour une description complète de la structure linkmonitoring.

MU-6.4.6 Configuration PAP

Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction au PAP.

Pour configurer PAP sur une liaison PPP(oA), procédez de la façon suivante:

Etape	Action
1	**Liaison PPP** Sur le routeur d'authentification, allez à l'objet ppp et configurez les attributs authentication et authenPeriod (voir ci-dessous). **Liaison PPPoA** sur le routeur d'authentification, allez à l'objet atm, sélectionnez pvcTable, puis sélectionnez la structure ppp et configurez les éléments authentication et authenPeriod (voir ci-dessous).  • authentication. Utilisez cet attribut pour définir l'authentification PPP sur PAP. • authenPeriod. Utilisez cet attribut pour déterminer l'intervalle selon lequel la liaison PPP est authentifiée après avoir été établie. Reportez-vous à MR-1.5.3 - PPP configuration attributes page 52 pour une description détaillée des attributs ppp.
2	Sur le routeur pair, configurez les attributs suivants: • sysName. Utilisez cet attribut pour définir le nom du pair. Il est utilisé dans le processus d'authentification. Sinon, vous pouvez utiliser l'attribut sessionName. Reportez-vous à MU-6.4.10 - Quels attributs de nom et de secret utiliser pour l'authentification PPP? page 137 sur de plus amples informations sur ce qu'il convient d'utiliser. • sysSecret. Utilisez cet attribut pour définir le secret du pair. Il est utilisé dans le processus d'authentification. Sinon, vous pouvez utiliser l'attribut sessionSecret. Reportez-vous à MU-6.4.10 - Quels attributs de nom et de secret utiliser pour l'authentification PPP? page 137 sur de plus amples informations sur ce qu'il convient d'utiliser.
3	Sur le routeur d'authentification, allez à l'objet router et configurez pppSecretTable. Dans cette table, entrez le nom et le secret que vous avez configurés sur le pair à l'étape 2. Ils sont utilisés dans le processus d'authentification. 

L'explication sur la manière exacte d'utiliser tous ces attributs de configuration se trouve dans MU-6.4.7 - Comment fonctionne le PAP? page 132.

MU-6.4.7 Comment fonctionne le PAP?

Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction au PAP.

Authentification PAP dans un sens

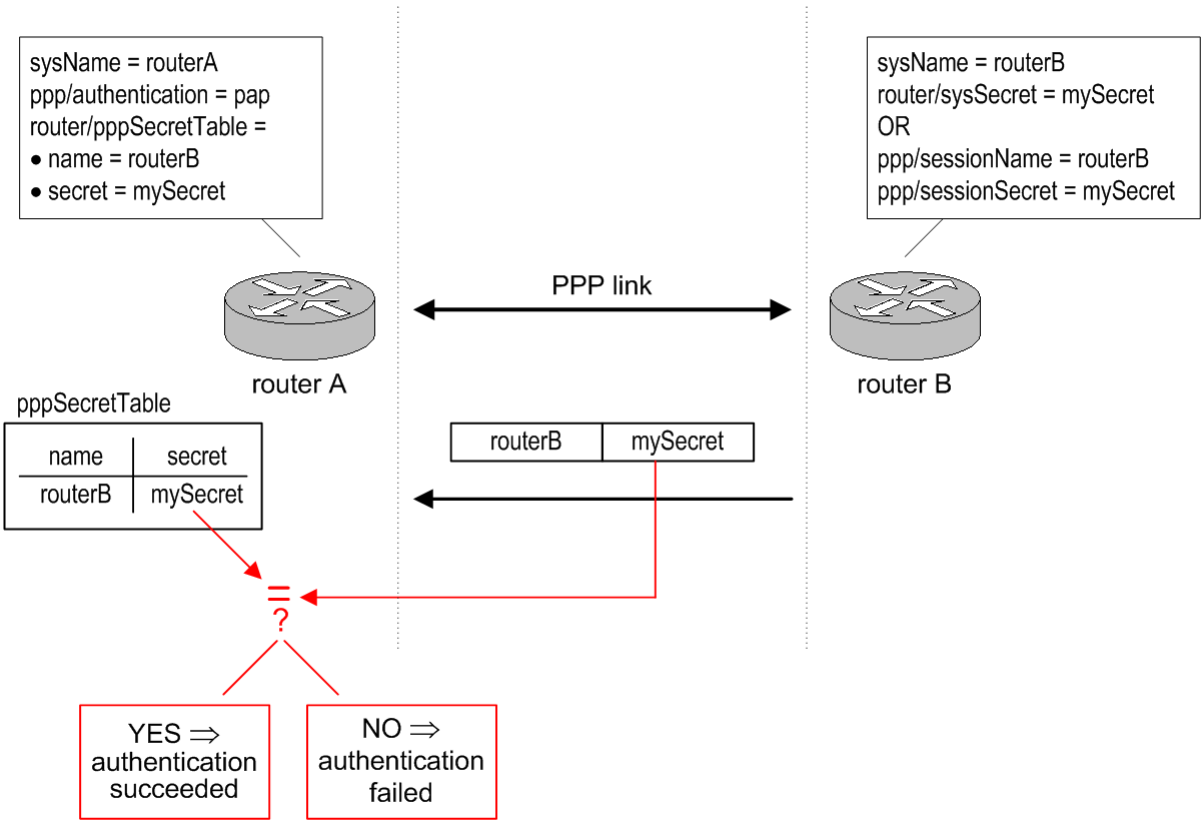
Le routeur authentifie après avoir configuré sa couche LCP et avant de configurer sa couche IPCP. Si l'authentification est réussie, la constitution de la liaison PPP se poursuit jusqu'à ce que les données puissent être envoyées. Sinon, le PPP recommence l'établissement de liaison.

Prenons l'exemple suivant: le routeur A (le Routeur Telindus 1421 SHDSL) est l'authentificateur et le routeur B le pair. Le routeur A est configuré pour l'authentification PAP, pas le routeur B. Le processus d'authentification se déroule de la manière suivante:

Phase	Description
1	Le routeur B veut établir une liaison PPP avec le routeur A (le Routeur Telindus 1421 SHDSL).
2	Le routeur A demande au routeur B de s'auto-authentifier.
3	Le routeur B envoie son nom[1] et son secret[2] au routeur A.
4	Le routeur A examine le nom du routeur B dans son pppSecretTable pour trouver un secret correspondant. Si le secret trouvé dans pppSecretTable correspond au secret reçu du routeur B, l'authentification est réussie et une liaison PPP est établie. Sinon, l'authentification a échoué et aucune liaison PPP n'est établie.

1. En fonction de la configuration du routeur B, ce peut être sont sysName ou sessionName.
2. En fonction de la configuration du routeur B, ce peut être sont sysSecret ou sessionSecret.

La figure suivante illustre le processus d'authentification PAP:



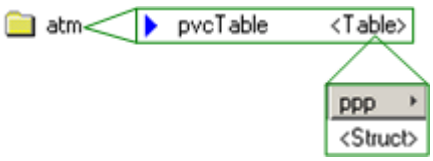
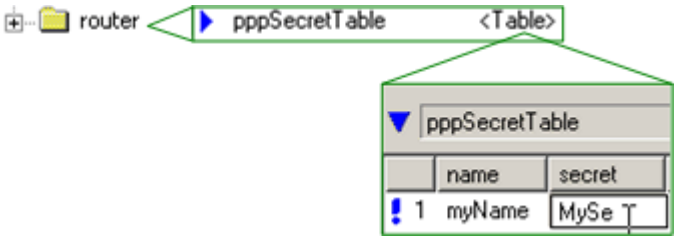
Authentification PAP dans les deux sens

Si l'authentification PAP est activée sur les deux routeurs, ils envoient tous les deux une demande et répondent à l'authentification. Si le routeur distant est un routeur d'une autre marque, lisez la documentation pour voir comment configurer le nom PAP et les valeurs de secret.

MU-6.4.8 Configuration CHAP

Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction au CHAP.

Pour configurer un CHAP sur une liaison PPP(oA), procédez de la façon suivante:

Etape	Action
1	**Liaison PPP** Sur le routeur d'authentification, allez à l'objet ppp et configurez les attributs authentication et authenPeriod (voir ci-dessous). **Liaison PPPoA** sur le routeur d'authentification, allez à l'objet atm, sélectionnez pvcTable, puis sélectionnez la structure ppp et configurez les éléments authentication et authenPeriod (voir ci-dessous).  • authentication. Utilisez cet élément pour définir l'authentification PPP du CHAP (ou MS-CHAP ou MS-CHAP v2). • authenPeriod. Utilisez cet attribut pour déterminer l'intervalle selon lequel la liaison PPP est authentifiée après avoir été établie. Reportez-vous à MR-1.5.3 - PPP configuration attributes page 52 pour une description détaillée des attributs ppp.
2	Sur le routeur pair, configurez les attributs suivants: • sysName. Utilisez cet attribut pour définir le nom du pair. Il est utilisé dans le processus d'authentification. Sinon, vous pouvez utiliser l'attribut sessionName. Reportez-vous à MU-6.4.10 - Quels attributs de nom et de secret utiliser pour l'authentification PPP? page 137 sur de plus amples informations sur ce qu'il convient d'utiliser. • sysSecret. Utilisez cet attribut pour définir le secret du pair. Il est utilisé dans le processus d'authentification. Sinon, vous pouvez utiliser l'attribut sessionSecret. Reportez-vous à MU-6.4.10 - Quels attributs de nom et de secret utiliser pour l'authentification PPP? page 137 sur de plus amples informations sur ce qu'il convient d'utiliser.
3	Sur le routeur d'authentification, allez à l'objet router et configurez pppSecretTable. Dans cette table, entrez le nom et le secret que vous avez configurés sur le pair à l'étape 2. Ils sont utilisés dans le processus d'authentification. 

L'explication sur la manière exacte d'utiliser tous ces attributs de configuration se trouve dans MU-6.4.9 - Comment fonctionne le CHAP? page 135.

MU-6.4.9 Comment fonctionne le CHAP?

Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction au CHAP.

Authentification CHAP dans un sens

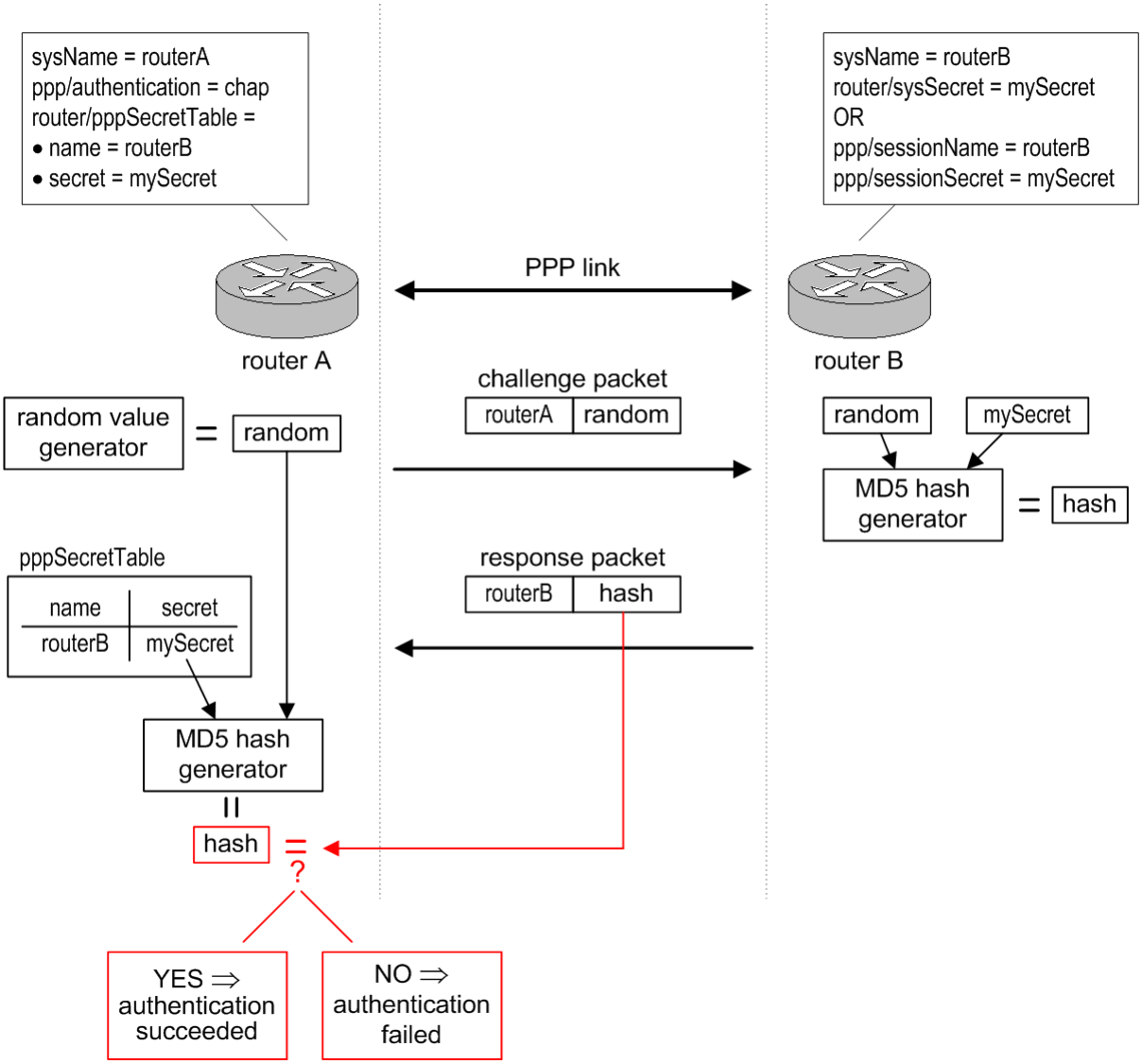
Le routeur authentifie après avoir configuré sa couche LCP et avant de configurer sa couche IPCP. Si l'authentification est réussie, la constitution de la liaison PPP se poursuit jusqu'à ce que les données puissent être envoyées. Sinon, le PPP recommence l'établissement de liaison.

Prenons l'exemple suivant: le routeur A (le Routeur Telindus 1421 SHDSL) est l'authentificateur et le routeur B le pair. Le routeur A est configuré pour l'authentification CHAP, pas le routeur B. Le processus d'authentification se déroule de la manière suivante:

Phase	Description
1	Le routeur B veut établir une liaison PPP avec le routeur A (le Routeur Telindus 1421 SHDSL).
2	Le routeur A demande au routeur B de s'auto-authentifier. Le routeur A envoie un paquet de contrôle contenant une valeur aléatoire au routeur B. Le paquet de contrôle contient également le sysName du routeur A. Si le pair (routeur B) est également un routeur Telindus, rien ne se passe. D'autres marques peuvent toutefois utiliser ce sysName pour déterminer quel secret utiliser lors du processus d'authentification. Vérifiez la documentation du fabriquant.
3	Le routeur B transmet la valeur aléatoire et son secret[1] dans le générateur MD5, donnant une valeur mêlée.
4	Le routeur B envoie un paquet de réponse contenant la valeur mêlée et son nom [2].
5	Le routeur A examine le nom du routeur B dans son pppSecretTable pour trouver un secret correspondant. Le secret trouvé dans pppSecretTable et la valeur aléatoire que le routeur A avait envoyée à l'étape 2 sont transmis au générateur MD5, donnant une valeur mêlée. Si cette valeur est égale à la valeur mêlée reçue du routeur B, l'authentification a réussi et une liaison PPP est établie. Sinon, l'authentification a échoué et aucune liaison PPP n'est établie.

1. En fonction de la configuration du routeur B, ce peut être sont sysSecret ou sessionSecret.
2. En fonction de la configuration du routeur B, ce peut être sont sysName ou sessionName.

La figure suivante illustre le processus d'authentification:



Authentification CHAP dans les deux sens

Si l'authentification CHAP est activée sur les deux routeurs, ils envoient tous les deux une demande et répondent à l'authentification. Si le routeur distant est un routeur d'une autre marque, lisez la documentation pour voir comment configurer le nom CHAP et les valeurs de secret.

MU-6.4.10 Quels attributs de nom et de secret utiliser pour l'authentification PPP?

Les anciennes versions du firmware utilisaient les attributs sysName et router/sysSecret lors de leur processus d'authentification PPP. Les nouvelles versions présentent deux nouveaux attributs pour l'authentification PPP, à savoir: ppp/sessionName et ppp/sessionSecret. Cette amélioration vous permet de définir des noms et des secrets différents pour chaque liaison PPP (alors qu'avant, toutes les liaisons PPP utilisaient le même attribut sysName et sysSecret).

Supposons que vous ayez plusieurs ATM PVC sur lesquels vous faites fonctionner PPPoA ; vous pouvez utiliser un nom et un secret différent pour chaque liaison PPPoA en configurant pour chaque PVC sessionName et sessionSecret dans la structure ppp de l'attribut atm/pvcTable.

Reportez-vous au…

- telindus1421Router/sysName page 14
- telindus1421Router/router/sysSecret page 87
- telindus1421Router/wanInterface/ppp/sessionName page 57
- telindus1421Router/wanInterface/ppp/sessionSecret page 57

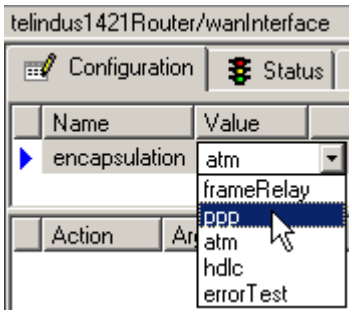
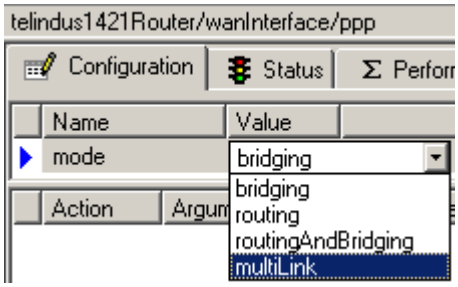
Remarques importantes

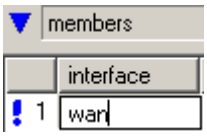
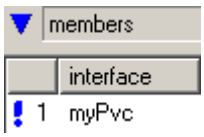
- Si l'authentification est activée sur une liaison PPP et si les attributs sessionName/sessionSecret ne sont *pas* complétés, les attributs sysName/sysSecret sont alors utilisés dans le processus d'authentification PPP pour cette liaison.
- Si l'authentification est activée sur une liaison PPP et si les attributs sessionName/sessionSecret sont complétés, les attributs sysName/sysSecret sont alors ignorés et ne sont *pas* utilisés lors du processus d'authentification PPP pour cette liaison.
- Si vous avez plusieurs liaisons PPP et si vous utilisez un nom et un secret différents pour chacune d'elles (en utilisant les attributs sessionName/sessionSecret), n'oubliez pas d'ajouter tous ces noms et secrets dans le pppSecretTable de l'authentificateur.
- Les attributs sysName/sysSecret ne servent pas de “sauvegarde” pour les attributs sessionName/sessionSecret. Cela signifie que si, pour une raison quelconque, l'authentification utilisant les attributs sessionName/sessionSecret échoue (p. ex. parce que les secrets ne correspondent pas), l'authentificateur ne redémarre *pas* le processus d'authentification en utilisant les attributs sysName/sysSecret à la place.
- Si vous avez plusieurs liaisons PPP, il est permis d'utiliser un nom et un secret spécifique sur certaines d'entre elles (en utilisant les attributs sessionName/sessionSecret) et d'utiliser un nom et un secret générique pour les autres (en utilisant les attributs sysName/sysSecret). Dans ce cas, assurez-vous que pour ces derniers, les attributs sessionName/sessionSecret sont *not* configurés (c'est-à-dire que leurs champs de valeur sont vides).

MU-6.4.11 Configuration de PPP multiliaisons

MLPPP signifie faire tourner un faisceau PPP sur plusieurs interfaces physiques. En cas de Routeur Telindus 1421 SHDSL, la configuration de MLPPP semble un peu difficile parce que le Routeur Telindus 1421 SHDSL n'a qu'une seule interface physique à destination du WAN. Toutefois, si vous souhaitez activer la fragmentation PPP ou établir des liaisons PPP multiclasses, vous devez configurer un faisceau PPP même si cela implique la configuration d'un faisceau sur une seule interface physique. Cela est dû au fait que la fragmentation PPP et le PPP multiclasses font partie des fonctions de MLPPP.

Pour configurer MLPPP, procédez de la manière suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet wanInterface et réglez l'attribut encapsulation sur ppp. 
2	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet wanInterface/ppp et réglez l'attribut mode sur multiLink. 
3	Créez un faisceau PPP. Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet bundle et ajoutez un objet pppBundle[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43). P. ex. pppBundle[myPppBundle]

Etape	Action
4	Configurez les attributs de l'objet pppBundle[ ] que vous venez d'ajouter. Les attributs les plus importants sont:: • members. Utilisez cet attribut pour faire de l'interface WAN un membre du faisceau PPP. Faites-le en ajoutant une entrée à la table members et en entrant “wan” comme valeur de l'élément interface.  • ip. Utilisez cet attribut pour configurer les paramètres de l'IP du faisceau PPP. • mode. Utilisez cet attribut pour déterminer si les paquets sont traités par le processus d'acheminement, de pontage ou les deux. Reportez-vous à MR-1.8.1 - PPP bundle configuration attributes page 74 pour de plus amples informations sur les attributs de configuration faisceau PPP. Notez que si vous faites tourner PPP sur un ATM (PPPoA), vous pouvez aussi créer des faisceaux PPP. Dans ce cas, il suffit d'entrer le nom de l'ATM PVC comme valeur de l'élément interface dans la table members. 

MU-6.4.12 Activation de la fragmentation PPP

Configurer un PPP multiliaisons (MLPPP) vous permet d'activer la fragmentation PPP. Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction à la fragmentation PPP.

Remarque importante

Notez que la fragmentation PPP fait partie des fonctions de MLPPP. Donc, si vous souhaitez activer la fragmentation PPP, vous devez configurer un faisceau PPP. Même si voulez activer la fragmentation PPP sur une seule interface !

Pour activer la fragmentation PPP, procédez de la façon suivante:

Etape	Action
1	Configurez MLPPP comme décrit dans MU-6.4.11 - Configuration de PPP multiliaisons page 138. Notez que si vous souhaitez activer la fragmentation PPP sur une seule interface, vous devez créer un faisceau PPP contenant un seul membre.
2	Dans l'objet pppBundle[ ] que vous avez créé à l'étape 1, réglez l'attribut fragmentation sur enabled.

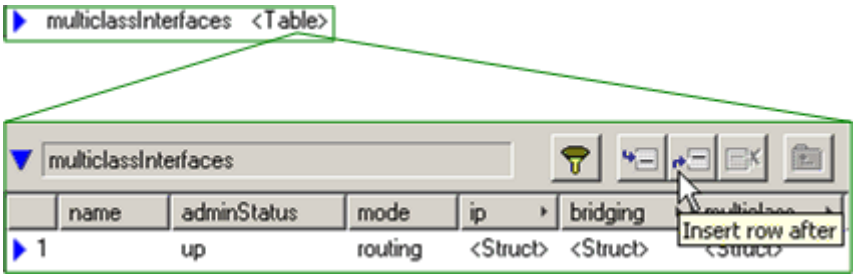
MU-6.4.13 Configuration de PPP multiclasses

Configurer un PPP multiliaisons (MLPPP) vous permet de configurer le PPP multiclasses. Reportez-vous à MU-6.4.1 - Introduction à PPP page 122 pour une introduction au PPP multiclasses.

Remarque importante

Notez que le PPP multiclasses fait partie des fonctions de MLPPP. Donc, si vous souhaitez activer un PPP multiclasses, vous devez configurer un faisceau PPP. Même si voulez activer le PPP multiclasses sur une seule interface !

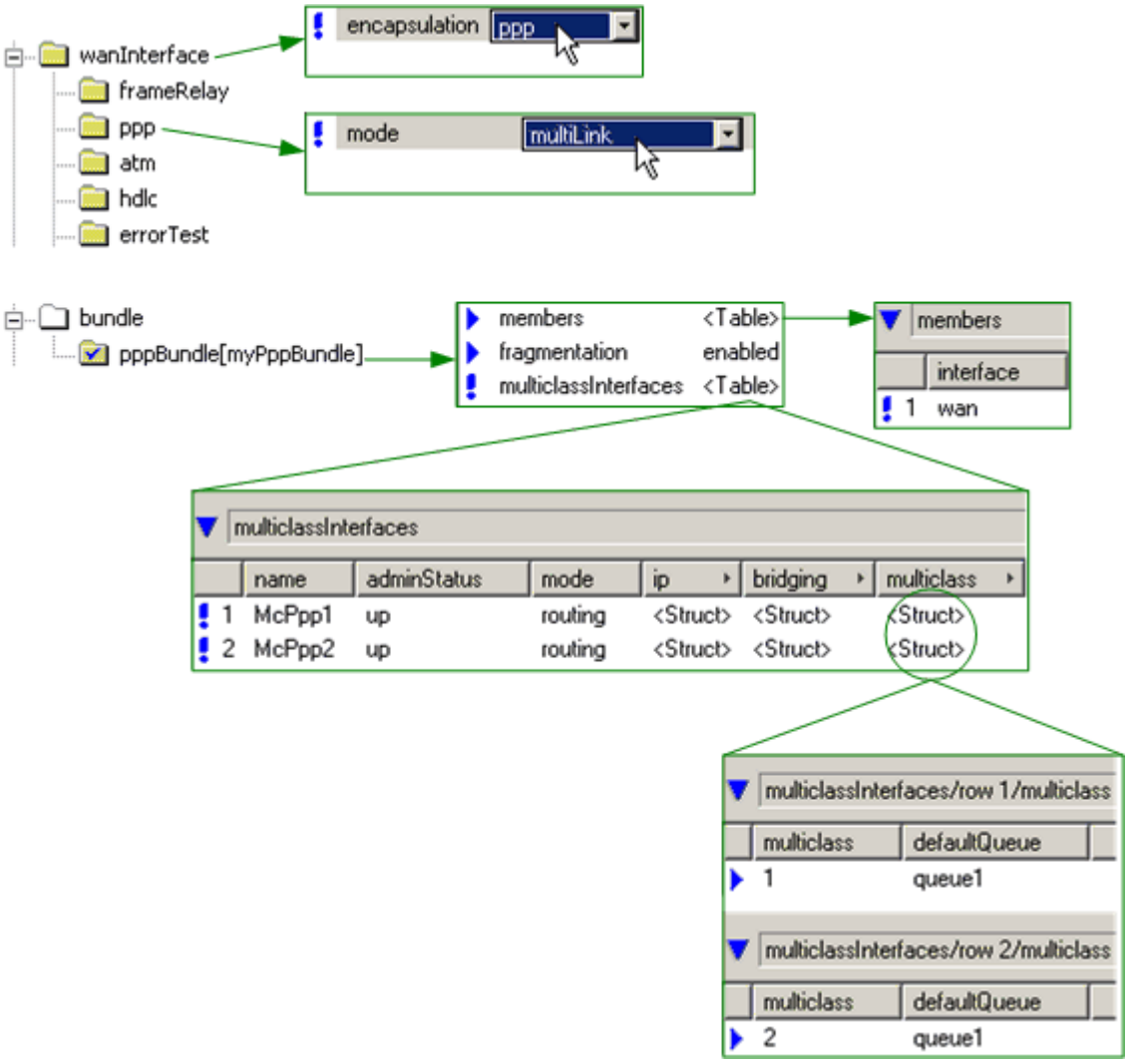
Pour configurer le PPP multiclasses, procédez de la façon suivante:

Etape	Action
1	Configurez MLPPP comme décrit dans MU-6.4.11 - Configuration de PPP multiliaisons page 138. Notez que si vous souhaitez activer le PPP multiclasses sur une seule interface, vous devez créer un faisceau PPP contenant un seul membre.
2	Dans l'objet pppBundle[ ] que vous avez créé à l'étape 1, sélectionnez l'attribut multiclassInterfaces et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour configurer les liaisons PPP. Ajoutez une ligne au tableau multiclassInterfaces pour chaque liaison PPP multiclasses que vous souhaitez créer.

Etape	Action
3	Configurez les éléments de la liaison PPP multiclasses que vous venez de créer. Ces éléments sont: • name. Utilisez cet élément pour assigner un nom administratif à la liaison PPP multiclasses. • adminStatus. Utilisez cet élément pour activer (up) ou désactiver (down) la liaison PPP multiclasses. • mode. Utilisez cet élément pour déterminer si, pour la liaison PPP multiclasses correspondante, les paquets sont traités par le processus d'acheminement, de pontage ou les deux. • ip. Utilisez cet élément pour configurer les paramètres de l'IP de la liaison PPP multiclasses. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour de plus amples informations. • bridging. Utilisez cet élément pour configurer les paramètres de pontage de la liaison PPP multiclasses si la liaison est en mode de pontage (c'est-à-dire si l'élément mode est réglé sur bridging). Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 pour de plus amples informations. • multiclass. Utilisez cet élément pour configurer les paramètres spécifiques de la liaison PPP multiclasses. L'élément multiclass contient les sous-éléments suivants: - multiclass. Utilisez cet élément pour régler un identificateur multiclasses pour la liaison PPP multiclasses. - defaultQueue. Utilisez cet élément pour sélectionner une file d'attente par défaut. Cela vous permet de configurer facilement une politique de trafic sans avoir à créer et à appliquer un profil de politique de trafic. Il vous reste encore à créer et à appliquer une politique de priorité pour vider la file. Reportez-vous à MU-7.8.9 - Attribut de la file par défaut ou profil de politique de trafic page 219 pour de plus amples informations. Reportez-vous à telindus1421Router/bundle/pppBundle[ ]/multiclassInterfaces page 76 pour une description détaillée de la table multiclassInterfaces.

Exemple – configuration de PPP multiclasses

Supposons que vous vouliez configurer 2 liaisons PPP multiclasses sur le WAN. Vous devez alors créer un faisceau PPP avec un seul membre, l'interface WAN, et configurer les attributs correspondants dans ce faisceau. Cela est illustré par la figure qui suit:



MU-6.5 Configuration d'encapsulation HDLC

Cette section présente le protocole d'encapsulation HDLC et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-6.5.1 - Introduction à HDLC page 145
- MU-6.5.2 - Configuration HDLC page 145

MU-6.5.1 Introduction à HDLC

L'encapsulation High-level Data Link Control (HDLC) signifie que les trames Ethernet sont placées dans une trame HDLC sans encapsulation supplémentaire (Frame Relay ou PPP). Cela signifie qu'aucun protocole ne surveille l'état de la liaison, mais aussi qu'il n'y a aucun en-tête d'encapsulation.

Les trames Ethernet étant directement encapsulées, seul le pontage est possible.

Remarque importante

L'encapsulation HDLC sur le Routeur Telindus 1421 SHDSL est compatible avec l'encapsulation HDLC sur l'interface Crocus Bridge. Elle n'est toutefois pas compatible avec l'encapsulation Cisco HDLC.

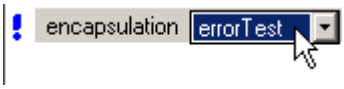
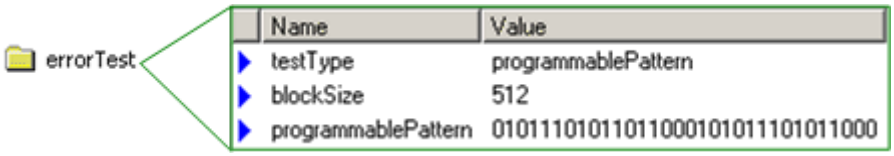
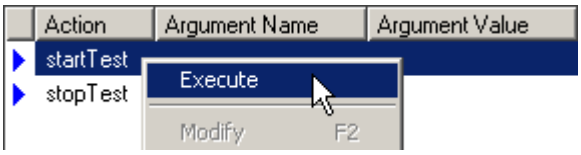
MU-6.5.2 Configuration HDLC

Pour l'encapsulation HDLC, seuls certains paramètres de pontage peuvent être configurés. Reportez-vous à telindus1421Router/wanInterface/hdlc/bridging page 59.

MU-6.6 Configuration d'un test d'erreur

Le Routeur Telindus 1421 SHDSL dispose d'un générateur / détecteur de motif de test d'erreur de couche 2 interne. Cette section explique comment configurer un test d'erreur.

Pour configurer un test d'erreur, procédez de la façon suivante:

Etape	Action
1	Réglez l'attribut encapsulation sur errorTest. 
2	Allez à l'objet errorTest, sélectionnez l'onglet Configuration et configurez les attributs suivants: • testType. Utilisez cet attribut pour sélectionner un motif de test. Si vous réglez l'attribut testType sur programmablePattern, vous pouvez générer votre propre motif de test en entrant un motif de test dans l'attribut programmablePattern (voir ci-dessous). • blockSize. Utilisez cet attribut pour définir la taille des blocs de test. • programmablePattern. Utilisez cet attribut pour générer votre propre motif de test. Pour ce faire, entrez un motif de test dans l'attribut programmablePattern et réglez l'attribut testType sur programmablePattern. 
3	Sélectionnez ensuite l'onglet Performance et exécutez l'action startTest. ⇒Le test démarre. Vous pouvez alors contrôler les résultats dans le groupe Status et le groupe Performance.  Vous pouvez également insérer des erreurs en exécutant l'action injectError.
4	Pour arrêter le test d'erreur, exécutez l'action stopTest. Vous pouvez alors effacer tous les compteurs en exécutant l'action executing the clearCounter.

MU-7 Configuration d'acheminement

Ce chapitre présente l'acheminement sur le Routeur Telindus 1421 SHDSL et répertorie les attributs que vous pouvez utiliser pour configurer l'acheminement. Outre cet acheminement, il présente par ailleurs les fonctions les plus importantes du routeur et répertorie les attributs que vous pouvez utiliser pour configurer ces fonctions.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.1 - Introduction à l'acheminement page 149
- MU-7.2 - Activation de l'acheminement sur une interface page 151
- MU-7.3 - Configuration de chemins statiques page 152
- MU-7.4 - Configuration d'acheminement en fonction de la politique page 161
- MU-7.5 - Configuration de RIP page 166
- MU-7.6 - Configuration OSPF page 177
- MU-7.7 - Configuration de translation d'adresses page 185
- MU-7.8 - Configuration de la politique de trafic et de priorité sur le routeur page 204

Reportez-vous au Manuel de référence pour un aperçu complet des attributs du Routeur Telindus 1421 SHDSL.

MU-7.1 Introduction à l'acheminement

Qu'est-ce que l'acheminement?

L'acheminement est le fait de déplacer les informations dans un réseau interne d'un point d'origine à un point de destination.

Acheminement ou pontage

L'acheminement est souvent mis en opposition au pontage. De prime abord, on pourrait dire que le pontage semble être la même chose que l'acheminement. La différence primaire entre les deux est que le pontage se produit sur la couche 2 (la couche de liaison) du modèle de référence OSI, alors que l'acheminement se produit sur la couche 3 (la couche réseau). En d'autres termes, le pontage se produit à un niveau inférieur et est par conséquent plus une fonction matérielle, alors que l'acheminement se produit à un niveau supérieur, auquel la composante logicielle est plus importante. L'acheminement intervenant à un niveau supérieur, il peut procéder à une analyse plus complexe pour déterminer le trajet optimal des paquets de données.

Activités d'acheminement de base

L'acheminement implique deux activités de base:

- la détermination des trajets d'acheminement optimum,
- le transport de groupes d'information (appelés typiquement des paquets).

Détermination du trajet d'acheminement optimum

Pour déterminer un trajet d'acheminement, les routeurs initialisent et entretiennent à jour des tables d'acheminement. Ces tables d'acheminement contiennent un grand nombre d'informations. Par exemple:

- Les associations destination/prochain saut indiquent à un routeur qu'une destination spécifique peut être atteinte de manière optimale en envoyant le paquet vers un routeur spécifique représentant le "prochain saut" vers la destination finale. Lorsqu'un routeur reçoit un paquet entrant, il vérifie l'adresse de destination et tente d'associer cette adresse à un prochain saut.
- Désirabilité d'un trajet. Les routeurs utilisent des métriques pour évaluer le trajet le mieux adapté à l'acheminement d'un paquet.

Les routeurs communiquent entre eux et entretiennent leurs tables d'acheminement par la transmission d'un grand nombre de messages. Le message d'actualisation d'acheminement est l'un de ces messages, qui se compose généralement de la totalité ou d'une partie d'une table d'acheminement. En analysant les mises à jour d'acheminement provenant de tous les autres routeurs, un routeur peut constituer une image détaillée de la topologie du réseau.

Transport de paquets

Dans la plupart des cas, un hôte détermine s'il doit envoyer un paquet à un autre hôte. Après avoir obtenu l'adresse d'un routeur par un moyen quelconque, l'hôte source envoie un paquet spécifiquement adressé à l'adresse physique d'un routeur (c'est-à-dire Media Access Control ou MAC), cette fois avec l'adresse de protocole (c'est-à-dire le réseau) de l'hôte de destination.

Pendant qu'il examine l'adresse de protocole de destination du paquet, le routeur détermine s'il sait ou ne sait pas comment transmettre le paquet au saut suivant. Si le routeur ne sait pas comment transmettre ce paquet, il le rejette. En revanche, s'il sait comment le transmettre, il modifie l'adresse de destination physique en celle du prochain saut et envoie le paquet.

Le prochain saut peut être l'hôte de destination finale. Dans le cas contraire, le prochain saut est habituellement un autre routeur, qui exécute la même procédure de décision de commutation. Au fur et à mesure que le paquet transite par le réseau internet, son adresse physique change, mais son adresse de protocole reste la même.

MU-7.2 Activation de l'acheminement sur une interface

Reportez-vous à MU-7.1 - Introduction à l'acheminement page 149 pour la présentation.

Pour chaque interface IP, vous pouvez déterminer si vous procédez à un acheminement, un pontage, ou les deux. Le tableau suivant montre, pour chaque interface IP, comment activer l'acheminement sur cette interface:

Interface	Comment activer l'acheminement?
Interface LAN	Réglez l'attribut mode sur routing ou routingAndBridging. L'attribut mode se trouve dans l'objet lanInterface: telindus1421Router/lanInterface/mode. **Remarque importante** Si vous réglez l'attribut de configuration telindus1421Router/lanInterface/mode sur bridging, alors le réglage de l'attribut de configuration telindus1421Router/lanInterface/ip est ignoré. Dans ce cas, si vous souhaitez gérer le Routeur Telindus 1421 SHDSL via IP, vous devez configurer une adresse IP dans l'objet bridgeGroup. telindus1421Router/bridge/bridgeGroup/ip.
VLAN sur l'interface LAN	Réglez l'élément mode sur routing ou routingAndBridging. L'élément mode se trouve dans la table vlan qui est située dans l'objet lanInterface: telindus1421Router/lanInterface/vlan/mode.
ATM PVC	Réglez l'élément mode sur routing ou routingAndBridging. L'élément mode se trouve dans la table pvcTable qui est située dans l'objet atm: telindus1421Router/wanInterface/atm/pvcTable/mode.
Liaison PPP	Réglez l'élément mode sur routing ou routingAndBridging. L'élément mode se trouve dans l'objet ppp: telindus1421Router/wanInterface/ppp/mode.
PVC relais trame	Réglez l'élément mode sur routing ou routingAndBridging. L'élément mode se trouve dans la table dlciTable qui est située dans l'objet frameRelay: telindus1421Router/wanInterface/frameRelay/dlciTable/mode.
Tunnel L2TP	Réglez l'élément mode sur routing ou routingAndBridging. L'élément mode se trouve dans la table l2tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/l2tpTunnels/mode.
Tunnel IPSEC L2TP	Réglez l'élément mode sur routing ou routingAndBridging. L'élément mode se trouve dans la table ipsecL2tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/ipsecL2tpTunnels/mode.

MU-7.3 Configuration de chemins statiques

Cette section présente l'acheminement statique et fournit une description rapide des attributs que vous pouvez utiliser pour configurer l'acheminement statique.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.3.1 - Introduction de l'acheminement statique page 153
- MU-7.3.2 - Configuration d'un trajet par défaut page 154
- MU-7.3.3 - Configuration de la table d'acheminement page 155
- MU-7.3.4 - Configuration de la table d'acheminement – méthodes empiriques page 158
- MU-7.3.5 - Principe de réacheminement page 160

MU-7.3.1 Introduction de l'acheminement statique

Acheminement statique ou dynamique

Le tableau qui suit précise les différences entre acheminement statique et acheminement dynamique:

Algorithme d'acheminement	Description
statique	Les algorithmes d'acheminement statique ne sont en réalité pas de réels algorithmes, mais plutôt des cartes de table établies par l'administrateur réseau avant le début de l'acheminement. Ces cartes ne changent pas, à moins que l'administrateur réseau ne les modifie. Les algorithmes d'acheminement statique fonctionnent bien dans des environnements où le trafic réseau est facilement prévisible et où la conception du réseau est relativement simple.
dynamique	Les systèmes d'acheminement statique ne pouvant répondre aux modifications survenant dans un réseau, ils sont généralement considérés non adaptés aux grands réseaux d'aujourd'hui, en constante évolution. La plupart de ces algorithmes d'acheminement actuels sont des algorithmes d'acheminement dynamique, qui s'adaptent aux changements survenant dans les réseaux en analysant les messages entrants de mise à jour d'acheminement. Si le message indique qu'une modification est intervenue dans le réseau, le logiciel d'acheminement recalcule les trajets et envoie des messages de mise à jour de nouveaux acheminements. Ces messages parcourent tout le réseau, invitant les routeurs à revoir leurs algorithmes et à modifier leurs tables d'acheminement en conséquence. Reportez-vous également à … • MU-7.5.1 - Introduction RIP page 167. • MU-7.6.1 - Introduction à OSPF page 178.
statique et dynamique	Les algorithmes d'acheminement dynamique peuvent être complétés par des trajets statiques lorsque cela paraît nécessaire. Un routeur de dernier recours (un routeur vers lequel sont envoyés tous les paquets non acheminables), par exemple, peut être spécifié comme faisant office de repositionnement de tous les paquets non acheminables, permettant ainsi de s'assurer que tous les messages sont au moins traités d'une manière ou d'une autre.

Qu'est-ce qu'un trajet par défaut?

Un trajet par défaut est un trajet (appelé également passerelle) utilisé pour diriger les paquets adressés aux réseaux non explicitement répertoriés dans la table d'acheminement. Un trajet par défaut est également typiquement utilisé lorsqu'un seul réseau distant spécifique doit être atteint.

Qu'est-ce qu'une table d'acheminement?

La table d'acheminement se compose d'un ensemble de trajets connus du routeur. Elle inclut une liste d'adresses connues, ainsi que des informations sur la manière d'obtenir un paquet sur un routeur plus proche de sa destination finale. Les tables d'acheminement peuvent être statiques (les trajets sont entrés manuellement par l'administrateur réseau) ou dynamiques (les routeurs communiquent entre eux pour échanger des informations de connexion et d'acheminement en utilisant, par exemple, RIP).

MU-7.3.2 Configuration d'un trajet par défaut

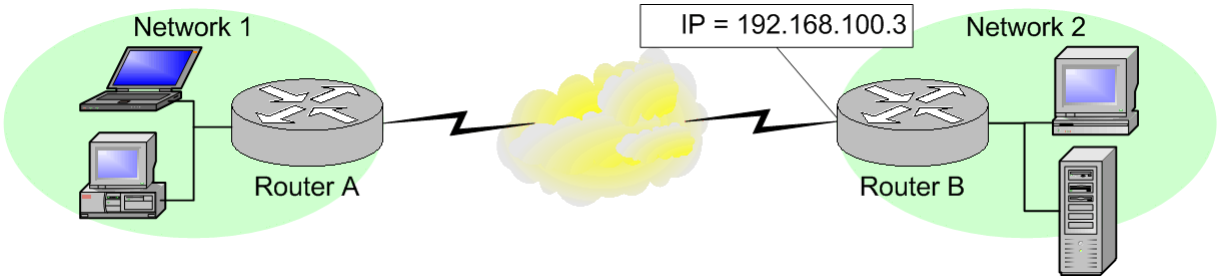
Reportez-vous à MU-7.3.1 - Introduction de l'acheminement statique page 153 pour une introduction sur les trajets par défaut.

Pour configurer un trajet par défaut, procédez de la manière suivante:

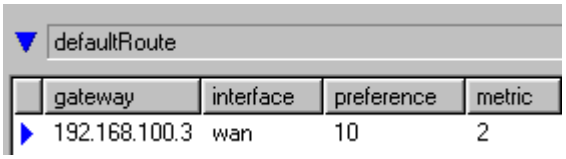
Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et sélectionnez l'attribut defaultRoute.
2	Configurez les éléments de la structure defaultRoute. Les éléments les plus importants sont: • gateway. Utilisez cet élément pour spécifier l'adresse IP du prochain routeur qui acheminera tous les paquets pour lesquels il n'existe aucun trajet (statique ou dynamique) spécifique dans la table d'acheminement. • interface. Utilisez cet élément pour spécifier l'interface grâce à laquelle la passerelle peut être atteinte. Pour ce faire, entrez le nom de l'interface telle que vous l'avez affectée en utilisant l'attribut de configuration name (p. ex. telindus1421Router/lanInterface/name). Notez que cette interface peut aussi être un DLCI, un PVC, un tunnel, etc. Reportez-vous à telindus1421Router/router/defaultRoute page 81 pour de plus amples informations.

Exemple - configuration d'un trajet par défaut

Supposons que le réseau 1 soit connecté par le réseau d'un opérateur au réseau 2. Le réseau 1 a uniquement besoin d'atteindre le réseau 2. Il suffit alors au routeur du réseau 1 de configurer un trajet par défaut à destination du réseau 2.



Configurez l'attribut defaultRoute du routeur A de la façon suivante:



MU-7.3.3 Configuration de la table d'acheminement

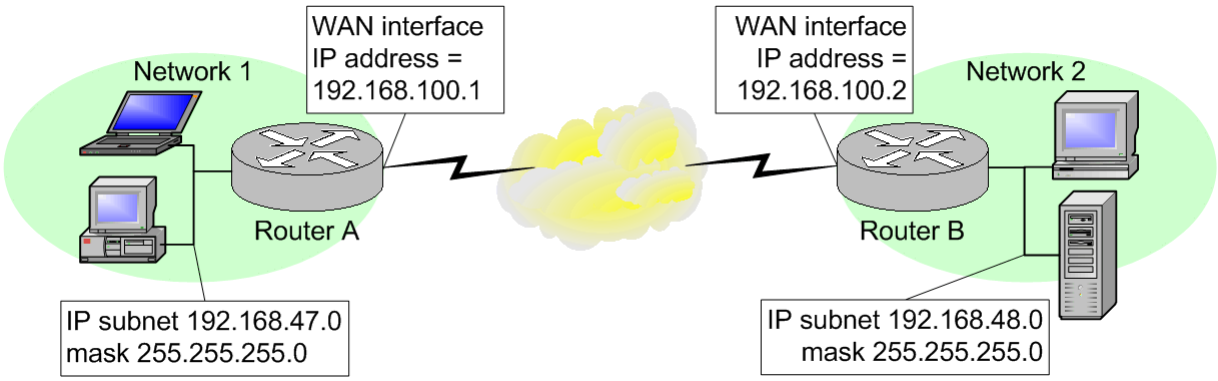
Reportez-vous à MU-7.3.1 - Introduction de l'acheminement statique page 153 pour une introduction sur la table d'acheminement.

Pour configurer la table d'acheminement, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et sélectionnez l'attribut routingTable.
2	Configurez les éléments de routingTable. • network. Utilisez cet élément pour spécifier l'adresse IP du réseau de destination. • mask. Utilisez cet élément pour spécifier le masque réseau du réseau de destination. • gateway. Utilisez cet élément pour spécifier l'adresse IP du prochain routeur sur le trajet vers le réseau de destination. • interface. Utilisez cet élément pour spécifier l'interface grâce à laquelle le réseau de destination peut être atteint. Pour ce faire, entrez le nom de l'interface telle que vous l'avez affectée en utilisant l'attribut de configuration name (p. ex. telindus1421Router/lanInterface/name). Notez que cette "interface" peut aussi être un DLCI, un PVC, un tunnel, etc. • preference. Utilisez cet élément pour définir le niveau d'importance du trajet par rapport aux trajets appris via RIP. Cet élément n'est important que lors de la combinaison de trajets statiques et de trajets RIP. • metric. Utilisez cet élément pour déterminer l'importance de l'incrémentation du paramètre métrique d'un trajet. Cet élément n'est important que lors de la combinaison de trajets statiques et de trajets RIP. Reportez-vous à telindus1421Router/router/routingTable page 82 pour de plus amples informations.

Exemple – configuration d'un trajet statique (adresse IP WAN disponible)

Supposons que le réseau 1 soit connecté par un réseau de l'opérateur au réseau 2. Les deux routeurs ont une adresse IP sur leur interface WAN.



Pour rendre le réseau 192.168.48.0 atteignable à partir du réseau 192.168.47.0 et vice versa, vous devez définir un trajet statique dans le routeur A et un trajet statique dans le routeur B. Configurez l'attribut routingTable des routeurs A et B de la manière suivante:

Router A :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.100.2		10	2

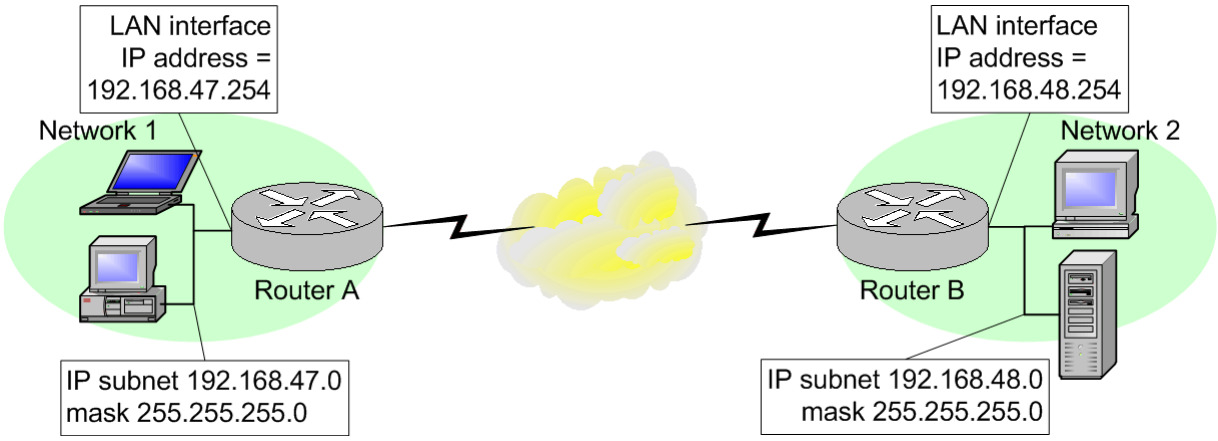
Router B :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.100.1		10	2

Exemple – configuration d'un trajet statique (adresse IP WAN non disponible)

Supposons que le réseau 1 soit connecté par un réseau de l'opérateur au réseau 2. Les deux routeurs n'ont aucune adresse IP sur leur interface WAN, seulement sur leur interface LAN.



Pour rendre le réseau 192.168.48.0 atteignable à partir du réseau 192.168.47.0 et vice versa, vous devez définir un trajet statique dans le routeur A et un trajet statique dans le routeur B. Configurez l'attribut routingTable des routeurs A et B de la manière suivante:

Router A :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.48.0	255.255.255.0	192.168.48.254	wan	10	2

Router B :

routingTable

	network	mask	gateway	interface	preference	metric
1	192.168.47.0	255.255.255.0	192.168.47.254	wan	10	2

MU-7.3.4 Configuration de la table d'acheminement – méthodes empiriques

Quelques-unes des règles applicables lors de la configuration de routingTable:

Règle	Description
1	De manière empirique, on peut dire que le nom de l'interface est prioritaire sur la passerelle.
2	Si vous entrez un nom d'interface correct (c'est-à-dire existant) et s'il fait référence à … • une interface point à point (PTP), le trajet est toujours ajouté à la table d'acheminement, quelle que soit la passerelle (GW) spécifiée. • une interface multipoints (MP), alors … - le trajet n'est ajouté à la table d'acheminement que si une passerelle locale est spécifiée. - le trajet n'est pas ajouté à la table d'acheminement lorsque aucune passerelle n'est spécifiée. - un réacheminement intervient lorsque aucune passerelle locale n'est spécifiée.
3	Si vous entrez un nom d'interface incorrect, le trajet n'est pas ajouté à la table d'acheminement.
4	Si vous n'entrez aucun nom d'interface, … • le trajet est ajouté à la table d'acheminement lorsque une passerelle locale est spécifiée. • le trajet n'est pas ajouté à la table d'acheminement lorsque aucune passerelle n'est spécifiée. • le trajet n'est pas ajouté à la table d'acheminement lorsque la passerelle se trouve dans le trajet de réseau configuré. Par exemple: réseau = 10.0.0.0; masque = 255.255.255.0; passerelle = 10.0.0.1. • un réacheminement intervient lorsque aucune passerelle locale n'est spécifiée.

Le tableau qui suit reprend ce qui a été dit plus haut:

Nom d'interface	Passerelle.	Résultat
correct	néant (0.0.0.0)	• PTP: trajet ajouté • MP: trajet non ajouté
correct	local	trajet ajouté (toujours)
correct	non local	• PTP: trajet ajouté [1] • MP: réacheminé
incorrect	-	trajet non ajouté
pas de nom	local pour une interface	trajet ajouté
pas de nom	non local pour une interface Exception: • GW = néant (0.0.0.0) • GW se trouve sur le trajet de réseau configuré	réacheminé vers passerelle • trajet non ajouté • trajet non ajouté

1. Dans l'état routingTable, la passerelle configurée apparaît, mais pour l'acheminement lui-même, la passerelle est ignorée.

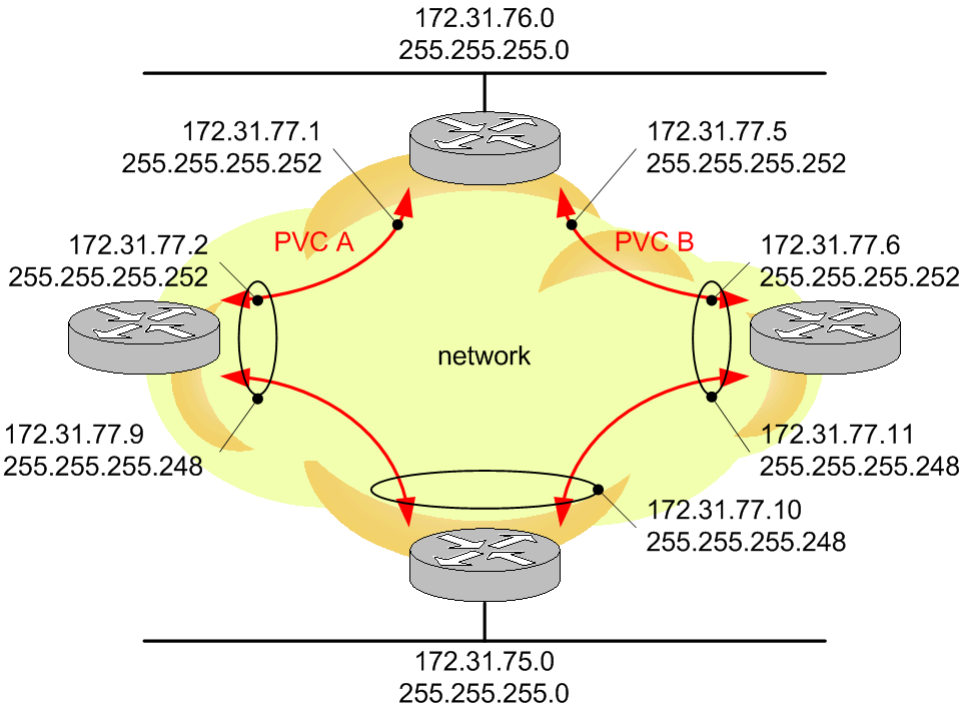
MU-7.3.5 Principe de réacheminement

Qu'est-ce que le principe de réacheminement?

Si la passerelle d'un trajet n'appartient pas au sous-réseau d'une interface, le Routeur Telindus 1421 SHDSL ajoute un trajet spécifique. Une recherche de second trajet se produit alors, cette fois en utilisant le champ de passerelle du trajet. Cela peut être utilisé comme une fonction de secours, comme illustré ci-après.

Exemple:

Supposons que vous ayez la configuration suivante:



Dans la table d'acheminement, les trajets suivants sont définis:

- le réseau 172.31.75.0 est joignable via 172.31.77.10
- 172.31.77.10 est joignable via PVC A (172.31.77.2)
- 172.31.77.10 est également joignable via PVC B (172.31.77.6)

routingTable

	network	mask	gateway	interface	preference	metric
1	172.31.75.0	255.255.255.0	172.31.77.10		10	2
2	172.31.77.10	255.255.255.248	172.31.77.2	wan	10	2
3	172.31.77.10	255.255.255.248	172.31.77.6	wan	10	2

Pour atteindre le réseau 172.31.75.0, la PVC A est utilisée. Toutefois, si la PVC A est déficiente, le Routeur Telindus 1421 SHDSL utilise automatiquement la PVC B pour atteindre le réseau 172.31.75.0. C'est-à-dire qu'il “réachemine” automatiquement, sans avoir besoin d'un protocole d'acheminement.

Remarques importantes

- Cela fonctionne uniquement pour les entrées de la table d'acheminement, *pas* pour la passerelle par défaut.
- Ce type de trajet est toujours actif.
- Dans les informations d'état, l'élément interface d'un tel trajet indique internal.

MU-7.4 Configuration d'acheminement en fonction de la politique

Cette section présente l'acheminement en fonction de la politique et fournit une description rapide des attributs que vous pouvez utiliser pour configurer cet acheminement.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.4.1 - Présentation de l'acheminement en fonction de la politique page 162
- MU-7.4.2 - Configuration de l'acheminement en fonction de la politique page 163

MU-7.4.1 Présentation de l'acheminement en fonction de la politique

Qu'est-ce que l'acheminement en fonction de la politique?

Un acheminement normal est basé sur l'adresse IP de destination. L'acheminement en fonction de la politique offre la possibilité de définir des entrées d'acheminement différentes en fonction d'informations complémentaires. Le trafic est acheminé vers une interface ou une passerelle donnée en fonction, par exemple, de l'adresse IP source, du protocole IP, etc.

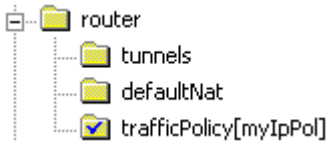
MU-7.4.2 Configuration de l'acheminement en fonction de la politique

Reportez-vous à MU-7.4.1 - Présentation de l'acheminement en fonction de la politique page 162 pour la présentation.

Pour configurer l'acheminement en fonction de la politique, procédez de la façon suivante:

<table>
<tr><th>Etape</th><th>Action</th></tr>
<tr><td>1</td><td>Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et ajoutez un objet trafficPolicy[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43).

p. ex. trafficPolicy[myIpPol]

 
</td></tr>
<tr><td>2</td><td>Sélectionnez une méthode de politique de trafic. Pour ce faire, utilisez l'attribut method dans l'objet trafficPolicy[ ] que vous avez ajouté à l'étape 1.

Dans le cas de l'acheminement en fonction de la politique, vous pouvez uniquement utiliser trafficShaping ou tosMapped, pas tosDiffServ.</td></tr>
<tr><td>3</td><td>Configurez les critères de politique de la méthode de trafic que vous avez sélectionnée à l'étape 2.

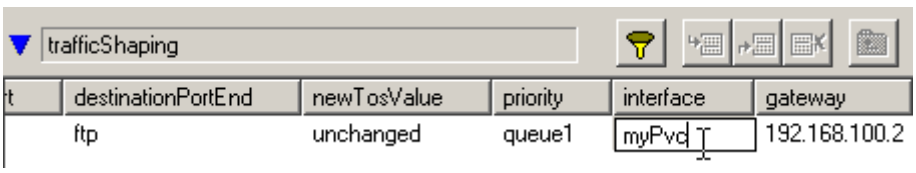
<table>
<tr><th>Si vous choisissez la méthode …</th><th>utilisez alors l'attribut suivant dans l'objet trafficPolicy[ ] pour configurer les critères de politique:</th></tr>
<tr><td>trafficShaping,</td><td>trafficShaping.

Ainsi, en utilisant les éléments de cette table, vous pouvez acheminer le trafic basé sur l'adresse IP de la source et de la destination, les valeurs TOS, le protocole IP, etc.</td></tr>
<tr><td>tosMapped,</td><td>tos2QueueMapping.

En utilisant les éléments de cette table, vous pouvez acheminer le trafic en fonction des valeurs TOS.</td></tr>
</table>

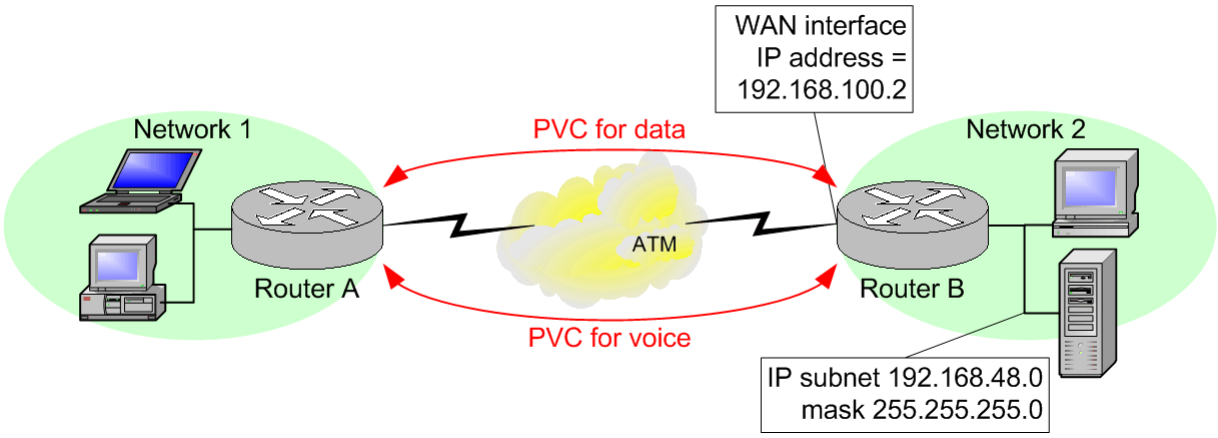
Pour de plus amples informations sur ces attributs, reportez-vous à …

• telindus1421Router/router/trafficPolicy[ ]/trafficShaping page 119.
• telindus1421Router/router/trafficPolicy[ ]/tos2QueueMapping page 124.</td></tr>
<tr><td>4</td><td>Vous devez maintenant déterminer vers quelle interface et quelle passerelle le trafic est acheminé. Pour ce faire, utilisez les éléments interface et gateway que vous trouvez dans les tables de politique de trafic que vous avez configurées à l'étape 3.

 
</td></tr>
</table>

Exemple - configuration d'acheminement en fonction de la politique

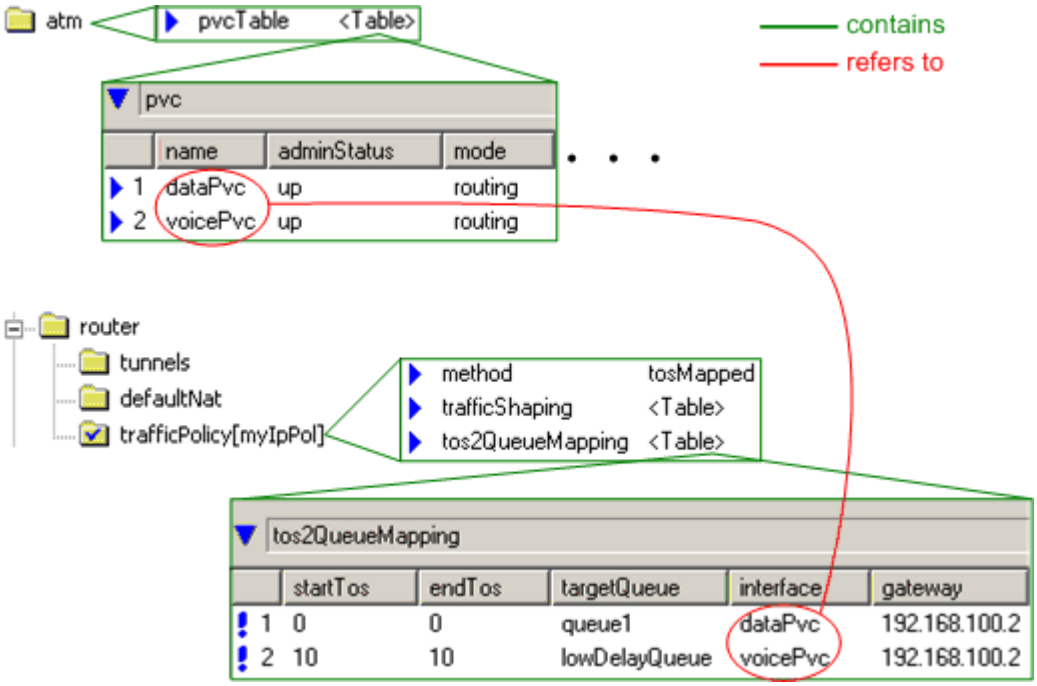
Supposons que vous disposiez de deux réseaux interconnectés par un réseau ATM. Le réseau 1 transporte un mélange de trafic de données et de trafic vocal. Le trafic présent sur ce réseau est différencié en réglant les valeurs Type Of Service (TOS) dans les en-têtes de paquets IP (données = 0, voix = 10). Lorsque le trafic est acheminé du réseau 1 au réseau 2, vous voulez que le trafic de données et le trafic vocal passent chacun par une PVC distincte.



A grands traits, voici comment configurer cette disposition:

Etape	Action
1	Configurez deux PVC ATM. Par exemple: • Configurez une PVC ATM qui transportera le trafic de données, p. ex. pvcTable/name = dataPvc. • Configurez une autre PVC ATM qui transportera le trafic vocal, p. ex. pvcTable/name = voicePvc. Puisque ce n'est pas le sujet principal de cet exemple, reportez-vous, pour de plus amples informations sur la création de PVC ATM, à MU-6.2.2 - Configuration d'ATM PVC page 91.
2	Créez et configurez une politique de trafic IP à des fins d'acheminement en fonction de la politique. Par exemple: • Créez un objet trafficPolicy[myIpPol]. • Réglez l'attribut method sur tosMapped. • Dans la table tos2QueueMapping, créez deux entrées et définissez les éléments startTos, endTos, interface et gateway de chaque entrée de telle manière que le trafic de données et le trafic vocal passent chacun par une PVC distincte.

La figure qui suit montre comment configurer l'acheminement en fonction de la politique:



MU-7.5 Configuration de RIP

Cette section présente le Routing Information Protocol (RIP) et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.5.1 - Introduction RIP page 167
- MU-7.5.2 - Activation RIP sur une interface page 168
- MU-7.5.3 - Explication de la structure rip page 171
- MU-7.5.4 - Activation de l'authentification RIP sur une interface page 176

MU-7.5.1 Introduction RIP

Qu'est-ce que le RIP?

Le Routing Information Protocol (RIP) est un protocole que les routeurs utilisent pour échanger des informations d'acheminement dynamique. Le RIP peut être activé ou désactivé sur chaque interface.

Il existe deux modes RIP principaux:

Mode RIP	Description
passif	Les mises à jour RIP reçues sont analysées, mais aucune n'est transmise.
active	Les mises à jour RIP sont transmises et reçues.

Comment fonctionne le RIP?

Lorsque RIP est activé, le Routeur Telindus 1421 SHDSL communique ses informations d'acheminement aux routeurs adjacents toutes les 30 secondes. Il reçoit également les informations d'acheminement provenant des routeurs adjacents. Grâce à ces informations, il adapte sa table d'acheminement de manière dynamique. Si aucune information sur un trajet donné n'a été reçue au bout de 180 secondes, ce trajet est déclaré *inactif*. Si, après 120 secondes supplémentaires (c'est-à-dire 300 secondes au total), aucune information n'est reçue sur ce trajet, il est alors effacé de la table d'acheminement.

Support RIP

Le Routeur Telindus 1421 SHDSL suppore le protocole RIP version 1, compatible 1 et 2. Le RIP version 1 est un protocole d'acheminement très courant. La version 2 inclut des fonctions supplémentaires, telles que les masques de sous-réseau variables et l'authentification. Vérifiez la version RIP utilisée par les autres routeurs du réseau.

Actuellement, le protocole d'acheminement RIPv2 nécessite l'emploi d'une adresse IP sur l'interface WAN.

Authentification RIP

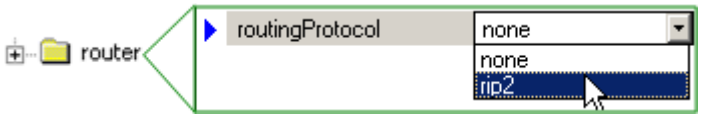
Pour des raisons de sécurité, les mises à jour RIP qui sont échangées entre les routeurs peuvent être authentifiées. L'authentification RIP peut être activée ou désactivée sur chaque interface.

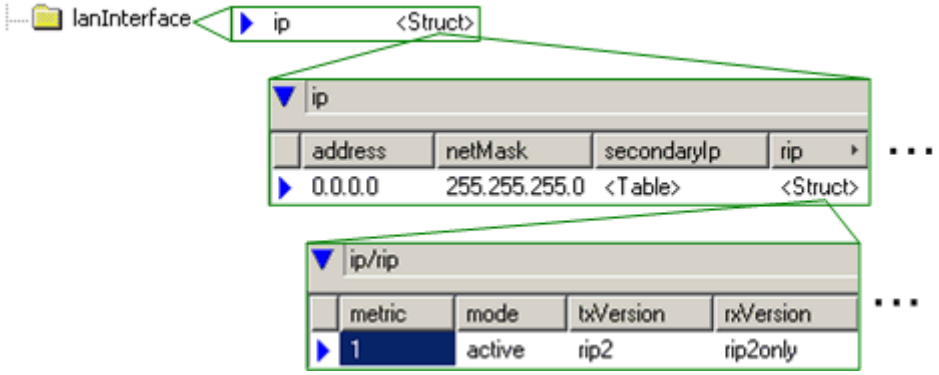
MU-7.5.2 Activation RIP sur une interface

Reportez-vous au…

- MU-7.3.1 - Introduction de l'acheminement statique page 153 pour une comparaison entre acheminement statique et dynamique (p. ex. utilisant RIP).
- MU-7.5.1 - Introduction RIP page 167 pour une introduction au RIP.

Pour activer l'acheminement dynamique en utilisant RIP sur une interface IP, procédez de la façon suivante:

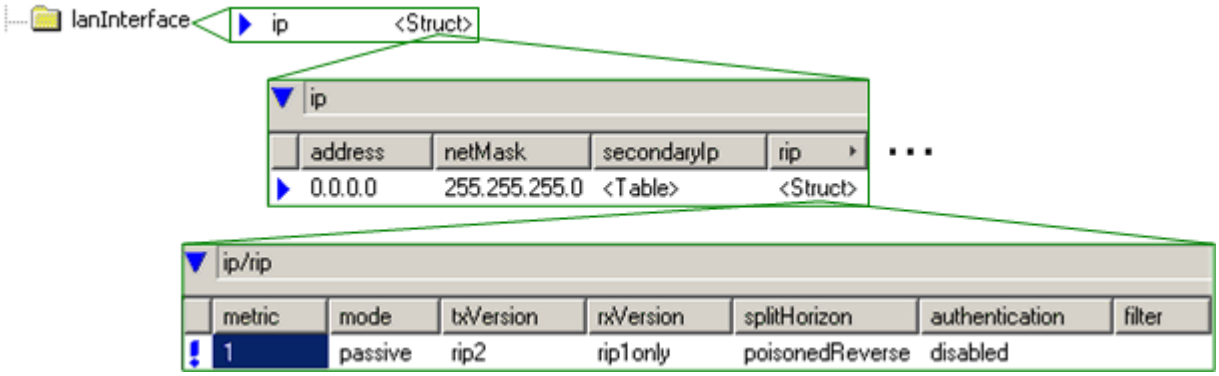
Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et réglez l'attribut routingProtocol sur rip.  Cela active le processus RIP général sur le Routeur Telindus 1421 SHDSL. Vous pouvez maintenant activer ou désactiver le RIP pour chaque interface IP. Notez que par défaut, RIP est activé sur toutes les interfaces IP.

Etape	Action
2	Chaque interface IP a une structure ip. Dans cette structure ip se trouve une structure rip. Utilisez les éléments suivants de la structure rip pour activer ou désactiver le RIP sur chaque interface IP: • mode. Utilisez cet élément pour régler la transmission et/ou la réception des mises à jour RIP sur l'interface. Par défaut, le Routeur Telindus 1421 SHDSL transmet et reçoit les mises à jour RIP sur toutes les interfaces. • txVersion. Utilisez cet élément pour définir la version des mises à jour RIP qui sont transmises sur l'interface. • rxVersion. Utilisez cet élément pour définir la version des mises à jour RIP reçues qui sont acceptées sur l'interface. Par exemple, les points qui suivent montrent l'emplacement de la structure rip sur l'interface LAN:  Reportez-vous au… • MU-5.2.2 - Où trouver les paramètres IP? page 54 pour l'emplacement de la structure ip sur les différentes interfaces IP. La structure rip est située dans la structure ip. • MU-7.5.3 - Explication de la structure rip page 171 pour une explication détaillée de la structure rip.

Exemple – configuration de RIP

Supposons que vous souhaitiez activer RIP sur l'interface LAN. De plus, vous souhaitez que cette interface LAN ne transmette pas les mises à jour RIP mais analyse uniquement les mises à jour RIP reçues (RIP passif). De surcroît, vous ne voulez accepter que les mises à jour du RIP version 1 sur l'interface LAN.

La figure qui suit vous montre comment procéder à la configuration:



Notez que, puisque dans cet exemple, l'élément mode est réglé sur passive, l'élément txVersion est ignoré.

MU-7.5.3 Explication de la structure rip

La structure rip survenant dans plusieurs objets, elle ne sera décrite ici qu'une seule fois et mentionnée lorsque cela sera nécessaire. La structure rip est située dans la structure ip. Reportez-vous à MU-5.2.2 - Où trouver les paramètres IP? page 54 pour l'emplacement de la structure ip.

La structure rip contient les éléments suivants:

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>métrique</td><td>Utilisez cet élément pour déterminer l'importance de l'incrémentation du paramètre métrique d'un trajet par le Routeur Telindus 1421 SHDSL.
Par défaut:1
Gamme:1 … 15

Les informations d'acheminement incluent un paramètre métrique. Chaque fois qu'un routeur est franchi, ce paramètre est incrémenté. De même, le Routeur Telindus 1421 SHDSL incrémente le paramètre métrique (par défaut, de 1) avant d'inscrire le trajet dans la table d'acheminement. Le paramètre métrique indique donc pour chaque trajet combien de routeurs doivent être franchis avant d'atteindre le réseau. Lorsqu'il existe plusieurs trajets vers un seul réseau et qu'ils ont tous les mêmes préférences, c'est le trajet présentant le plus petit paramètre métrique qui est alors choisi.

Toutefois, en utilisant l'élément metric, vous pouvez incrémenter le paramètre métrique de plus de 1 (jusqu'à un maximum de 15). Vous pouvez le faire, par exemple, pour indiquer qu'une interface donnée est moins souhaitable pour l'acheminement. En conséquence, le Routeur Telindus 1421 SHDSL ajoute cette valeur au paramètre métrique de chaque trajet appris par cette interface.

Le paramètre métrique est également utilisé pour représenter les sous-réseaux directement connectés sur les interfaces LAN et WAN.</td></tr>
<tr><td>mode</td><td>Utilisez cet élément pour régler la transmission et/ou la réception des mises à jour RIP sur l'interface. Par défaut, le Routeur Telindus 1421 SHDSL transmet et reçoit les mises à jour RIP sur toutes les interfaces.
Par défaut:actif
Gamme:énumérée, voir ci-

L'élément mode a les valeurs suivantes:

<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>active</td><td>Les mises à jour RIP sont transmises et reçues sur cette interface.</td></tr>
<tr><td>passif</td><td>Les mises à jour RIP ne sont pas transmises sur cette interface, mais les mises à jour reçues sont analysées.</td></tr>
<tr><td>disabled</td><td>Les mises à jour RIP ne sont ni transmises ni reçues sur cette interface.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>txVersion</td><td>Utilisez cet élément pour définir la version des mises à jour RIP qui sont transmises sur l'interface.
Par défaut:rip2
Gamme:énumérée, voir ci-

L'élément txVersion a les valeurs suivantes:

<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>rip1</td><td>Les mises à jour RIP transmises sont les mises à jour RIP version 1.</td></tr>
<tr><td>rip2</td><td>Les mises à jour RIP transmises sont les mises à jour RIP version 2.</td></tr>
<tr><td>compatible rip1</td><td>Le contenu du paquet de mise à jour RIP est un paquet RIP version 2, mais il est encapsulé comme un paquet RIP version 1. Cela permet à d'anciennes applications de RIP 1 d'être interopérables avec RIP 2.</td></tr>
</table></td></tr>
<tr><td>rxVersion</td><td>Utilisez cet élément pour définir la version des mises à jour RIP reçues qui sont acceptées sur l'interface.
Par défaut:rip2only
Gamme:énumérée, voir ci-

L'élément rxVersion a les valeurs suivantes:

<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>rip1only</td><td>Seules sont acceptées les mises à jour RIP version 1 reçues.</td></tr>
<tr><td>rip2only</td><td>Seules sont acceptées les mises à jour RIP version 2 reçues.</td></tr>
<tr><td>rip1&2</td><td>Les mises à jour RIP version 1 et 2 reçues sont acceptées.</td></tr>
</table>
Si vous souhaitez accepter des mises à jour compatibles RIP1 sur l'interface, réglez l'attribut rxVersion sur rip1&2.</td></tr>
</table>

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>splitHorizon</td><td>Utilisez cet élément pour activer ou désactiver le mode horizon partagé.
Par défaut:poisonedReverse
Gamme:énumérée, voir ci-

L'élément splitHorizon a les valeurs suivantes:

<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>disabled</td><td>Split horizon est désactivé.</td></tr>
<tr><td>enabled</td><td>Split horizon est activé.

Le mode Split horizon empêche que des informations d'acheminement ne sortent de l'interface par laquelle les informations ont été reçues en premier lieu. Ceci optimise les communications entre plusieurs routeurs, en particulier lorsque les liaisons sont interrompues. Il empêche également les boucles d'acheminement.</td></tr>
<tr><td>poisonedReverse</td><td>Poisoned reverse split horizon est utilisé.

Alors qu'un horizon partagé “simple” omet simplement les trajets appris dans les mises à jour envoyées à un voisin, l'horizon partagé poisoned reverse inclut ces trajets dans les mises à jour, mais règle leur métrique sur l'infini.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Elément</th><th>Description</th></tr>
<tr><td>authentification</td><td>Utilisez cet attribut pour activer ou désactiver l'authentification RIP.
Par défaut:désactivé
Gamme:énumérée, voir ci-

Reportez-vous à MU-7.5.4 - Activation de l'authentification RIP sur une interface page 176 pour de plus amples informations sur l'authentification RIP.

L'élément authentication a les valeurs suivantes:

<table>
<tr><th>Valeur</th><th>Description</th></tr>
<tr><td>disabled</td><td>Aucune authentification n'est utilisée.</td></tr>
<tr><td>texte</td><td>Le secret d'authentification est échangé en texte clair.</td></tr>
<tr><td>md5</td><td>Au lieu d'envoyer le secret d'authentification en même temps que les mises à jour RIP, il est mélangé avec les informations d'acheminement pour ne former qu'une seule valeur. Cette authentification est la plus sure. Elle protège également contre toute confusion avec le contenu d'un paquet: un mot de passe incorrect et des informations d'acheminement modifiées entraînent des valeurs différentes.</td></tr>
</table>

Remarques

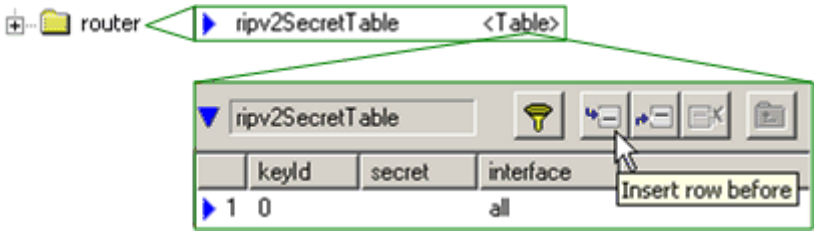
•Si l'authentification est activée (text ou md5), seules les mises à jour utilisant cette authentification sont traitées. Toutes les autres mises à jour de cette interface sont rejetées.
• Si vous utilisez md5 et si, pour une interface donnée, plusieurs secrets sont présents dans ripv2SecretTable, la première entrée dans ripv2SecretTable est utilisée pour transmettre les mises à jour RIP. L'authentification des mises à jour RIP reçues se fait en recherchant le premier secret avec un code correspondant.
• Si vous utilisez text et si, pour une interface donnée, plusieurs secrets sont présents dans ripv2SecretTable, la première entrée dans ripv2SecretTable est utilisée pour transmettre et recevoir les mises à jour RIP.</td></tr>
</table>

Elément	Description
filtre	Utilisez cet élément pour appliquer un filtre aux mises à jour RIP sur l'interface. Par défaut:<néant> Gamme:0 … 24 caractères Pour ce faire, entrez le nom d'indice du filtre que vous souhaitez utiliser. Vous pouvez créer le filtre lui-même en ajoutant un objet routingFilter sous l'objet router et en configurant les attributs dans cet objet. **Exemple:** Si vous avez créé un objet routingFilter portant le nom d'indice my_filter (c'est-à-dire routingFilter[my_filter]) et que vous souhaitiez appliquer ce filtre ici, entrez le nom d'indice comme valeur de l'élément filter. Reportez-vous au… • MR-1.9.5 - Routing filter configuration attributes page 114 pour de plus amples informations sur le filtrage RIP. • MU-4.4 - Ajout d'un objet dans l'arborescence page 43 pour de plus amples informations sur l'ajout d'objets.

MU-7.5.4 Activation de l'authentification RIP sur une interface

Reportez-vous à MU-7.5.1 - Introduction RIP page 167 pour une introduction à l'authentification RIP.

Pour activer l'authentification RIP sur une interface donnée, procédez de la façon suivante:

Etape	Action
1	Dans la structure rip, réglez l'élément authentification sur … • text. L'authentification RIP est activée et le secret d'authentification est envoyé en même temps que les mises à jour RIP en texte clair. • md5. L'authentification RIP est activée et le secret d'authentification est mélangé aux informations d'acheminement en une valeur unique. Reportez-vous à MU-7.5.3 - Explication de la structure rip page 171.
2	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router, sélectionnez l'attribut dhcpStatic et ajoutez une ou plusieurs entrées à cette table. 
3	Configurez les éléments d'une entrée dans l'attribut ripv2SecretTable: • keyId. Utilisez cet élément pour définir un identificateur unique pour chaque secret. • secret. Utilisez cet élément pour définir le secret. Ce secret est envoyé avec les mises à jour RIP sur l'interface spécifiée. Il est également utilisé pour authentifier les mises à jour RIP entrantes. • interface. Utilisez cet élément pour spécifier sur quelle interface le secret est utilisé. Pour ce faire, entrez le nom de l'interface telle que vous l'avez affectée en utilisant l'attribut de configuration name (p. ex. telindus1421Router/lanInterface/name). Notez que l' “interface” peut aussi être un e DLCI, un PVC, un tunnel, etc. Entrer la chaîne “all” (par défaut) signifie que le secret est utilisé sur toutes les interfaces. Reportez-vous à telindus1421Router/router/ripv2SecretTable page 86 pour de plus amples informations.

MU-7.6 Configuration OSPF

Cette section présente le protocole OSPF. Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.6.1 - Introduction à OSPF page 178
- MU-7.6.2 - Activation OSPF page 182
- MU-7.6.3 - Activation de l'authentification OSPF page 183

MU-7.6.1 Introduction à OSPF

Qu'est-ce que l'OSPF?

Le protocole Open Shortest Path First (OSPF) est un protocole Interior Gateway utilisé pour distribuer les informations d'acheminement dans un seul système autonome.

Sur l'internet, un système autonome (AS) est soit un réseau isolé, soit un groupe de réseaux contrôlé par un administrateur réseau commun (ou un groupe d'administrateurs) pour le compte d'une seule entité administrative (université, entreprise commerciale, division). Un système autonome est également parfois désigné sous l'appellation de domaine d'acheminement.

A l'aide de OSPF, un hôte qui reçoit une modification dans une table d'acheminement ou détecte une modification dans le réseau diffuse immédiatement les informations à tous les autres hôtes du réseau, afin que tous disposent des mêmes informations dans la table d'acheminement. Contrairement au RIP, dans lequel toute la table d'acheminement est envoyée, l'hôte qui utilise l'OSPF envoie uniquement la partie modifiée. Avec RIP, la table d'acheminement est envoyée à un hôte voisin toutes les 30 secondes. OSPF multidiffuse les informations actualisées uniquement lorsqu'une modification est survenue.

Que sont les états de liaison OSPF?

Plutôt que de simplement compter le nombre de sauts, l'OSPF base ses descriptions de trajet sur les "états de liaison" qui prennent en compte les informations de réseau supplémentaires. C'est la raison pour laquelle l'OSPF est appelé protocole d'état de liaison. Une liaison peut être considérée comme une interface sur le routeur. L'état de la liaison est une description de cette interface et de ses relations avec les routeurs voisins. Une description de l'interface comprend, par exemple, l'adresse IP de l'interface, le masque, le type de réseau auquel elle est connectée, les routeurs connectés à ce réseau, etc.

Chaque routeur du système autonome envoie un ou plusieurs messages d'état de liaison (LSA). L'ensemble de ces LSA constitue la base de données d'état de liaison. Chaque type de LSA a une fonction distincte. Il existe 4 types de LSA*:*

Paquets d'état de liaison	**Description**
LSA de routeur	• Décrivent l'état et le coût des liaisons des routeur (interfaces) dans le domaine, c'est-à-dire à l'intérieur du domaine. • Chaque routeur génère un LSA de routeur pour l'ensemble de ses interfaces.
LSA de réseau	Les LSA de réseau sont générés par un routeur désigné (DR) sur un segment. Ces informations sont une indication de tous les routeurs connectés à un segment multi-accès spécifique tel que Ethernet, Token Ring et FDDI (les DR seront examinés en détail par la suite).

Paquets d'état de liaison	Description
LSA condensés	• Les LSA condensés sont un moyen de condenser les informations d'acheminement d'un secteur. • Les LSA condensés décrivent les réseaux dans le système autonome, mais en-dehors d'une zone. Les liaisons condensées sont générées par un Area Border Router (ABR). Les ABR seront examinés par la suite. • En générant des liaisons condensées, les informations d'atteignabilité du réseau sont partagées entre les zones. Normalement, toutes les informations sont injectées dans l'ossature (zone 0), qui les transmet ensuite aux autres zones. Les ABR sont également chargés de diffuser les caractéristiques de liaison de l'ASBR. C'est le moyen par lequel les routeurs savent comment atteindre des trajets externes dans d'autres systèmes autonomes.
LSA AS externes	• Les LSA AS externes permettent de communiquer de manière transparente les informations d'acheminement externes dans le système autonome • Les LSA AS externes sont une indication des réseaux situés en-dehors de l'AS. Ces réseaux sont injectés dans l'OSPF par redistribution. Les liaisons externes sont générées par un ASBR (les ASBR seront examinés par la suite). L'ASBR est chargé d'injecter ces trajets dans un système autonome.

Qu'est-ce que le domaine d'ossature, ou ossature 0?

L'OSPF présente des restrictions spécifiques lorsque plusieurs domaines sont concernés. Si plus d'un domaine est configuré, l'un d'eux doit être le domaine 0. Il s'agit de l'ossature. Lors de la conception de réseaux, il est bon de commencer avec le domaine 0, puis de passer à d'autres domaines.

L'ossature doit être au centre de tous les autres domaines, c'est-à-dire que tous les domaines doivent être physiquement liés à l'ossature. La logique qui sous-tend cette structure est que l'OSPF s'attend à ce que tous les domaines injectent des informations d'acheminement dans l'ossature et qu'à son tour, celle-ci envoie les informations à d'autres domaines.

Que sont les domaines et les routeurs de limite?

L'OSPF utilise l'inondation pour échanger les mises à jour d'état de liaison entre les routeurs. Tout changement dans les informations d'acheminement est transmis à tous les autres routeurs du réseau. Les domaines sont introduits pour mettre une limite à l'explosion de ces mises à jour d'état de liaison. Tous les routeurs situés dans un domaine ont la même base de données d'état de liaison.

Un routeur qui a toutes ses interfaces dans le même domaine est appelé *routeur interne (IR)*.

Les routeurs qui appartiennent à plusieurs domaines et connectent ceux-ci à l'ossature sont appelés *routeurs de limite de domaine (ABR)*. Les ABR doivent donc conserver les informations décrivant les domaines d'ossature et les autres domaines connectés.

Les routeurs faisant office de passerelles (redistribution) entre l'OSPF et les autres protocoles d'acheminement (p. ex. RIP) sont appelés *routeurs de limite de système autonomes (ASBR)*.

Pour minimiser la quantité d'informations échangées sur un segment particulier, l'OSPF choisit un routeur comme *routeur désigné (DR)*, et un routeur comme *routeur désigné de secours (BDR)*, sur chaque segment à accès multiples. Le BDR est choisi comme mécanisme de secours pour le cas où le DR tomberait en panne (le DR et le BDR sont choisis en fonction de leur priorité OSPF). L'idée qui sous-tend cela est que les routeurs ont un point central de contact pour l'échange d'informations. Au lieu d'avoir chaque routeur échangeant des mises à jour avec chaque autre routeur sur le segment, chaque routeur échange des informations avec le DR et le BDR. Le DR et le BDR relaient les informations vers les autres.

Que sont les domaines souches?

L'OSPF permet à certains domaines d'être configurés comme domaines souches. Les réseaux externes, tels que ceux redistribués à partir d'autres protocoles dans l' OSPF, ne peuvent être inondés dans un domaine souche. L'acheminement à partir de ces domaines vers l'extérieur est basé sur un trajet par défaut. Configurer un domaine souche réduit la taille de la base de données topologique à l'intérieur d'un domaine et réduit les besoins de mémoire des routeurs situés à l'intérieur de ce domaine.

Un domaine peut être appelé souche dès lors qu'existe un point de sortie unique à partir de ce domaine ou si l'acheminement vers l'extérieur du domaine ne passe pas par un trajet optimal. La dernière description est juste une indication qu'un domaine souche ayant plusieurs points de sortie voit un ou plusieurs routeurs de limite de domaine injecter une valeur par défaut dans ce domaine.

Tous les routeurs OSPF situés dans un domaine souche doivent être configurés comme routeurs souches. Cela est dû au fait que dès lors qu'un domaine est configuré comme souche, toutes les interfaces appartenant à ce domaine commencent à échanger des paquets d'identification avec un fanion qui indique que l'interface est une souche. Tous les routeurs ayant un segment commun doivent accepter ce fanion. Dans le cas contraire, ils ne deviennent pas voisins et l'acheminement n'a pas lieu.

Que signifie voisins et adjacents?

Les routeurs qui partagent un segment commun deviennent *voisins* sur ce segment. Les voisins sont découverts par le protocole Hello. Les paquets Hello sont envoyés périodiquement à partir de chaque interface utilisant la multidiffusion IP. Les routeurs deviennent voisins dès qu'ils se voient répertoriés dans le paquet Hello du voisin. De cette manière, une communication bidirectionnelle est assurée.

Adjacents est l'étape suivante après la procédure de voisinage. Les routeurs adjacents sont les routeurs qui vont au-delà du simple échange Hello et poursuivent par le processus d'échange de base de données. Pour minimiser la quantité d'informations échangées sur un segment donné, l'OSPF choisit un routeur comme routeur désigné (DR) et un routeur comme routeur désigné de secours (BDR), sur chaque segment à accès multiple (reportez-vous à Que sont les domaines et les routeurs de limite? page 179).

Qu'est-ce que le coût OSPF?

Le coût d'une interface dans OSPF est une indication de la marge requise pour envoyer les paquets sur une interface donnée. Le coût d'une interface est inversement proportionnel à la largeur de bande de cette interface. Une largeur de bande supérieure indique un coût moins élevé. La marge (coût supérieur) et la temporisation impliquées pour le franchissement d'une ligne série à 56k sont plus importante que pour franchir une ligne Ethernet à 10M.

Le coût d'une interface peut être calculé automatiquement, ou l'utilisateur peut omettre le coût calculé en utilisant sa propre configuration, afin que la préférence soit accordée à certains trajets.

La formule utilisée pour calculer le coût est la suivante:

coût = largeur de bande de référence (en bps) / largeur de bande d'interface (en bps)

La *largeur de bande de référence* peut être définie par l'utilisateur.

Liaisons virtuelles

Les liaisons virtuelles sont utilisées à deux fins:

- La liaison d'un domaine qui n'a pas de connexion physique avec l'ossature.
- La correction de l'ossature en cas de discontinuité du domaine 0.

Comme nous l'avons vu plus haut, le domaine 0 doit se trouver au centre de tous les autres domaines. Dans certains cas rares où il est impossible d'avoir un domaine physiquement connecté à l'ossature, on utilise une liaison virtuelle. La liaison virtuelle assure au domaine non connecté un trajet logique jusqu'à l'ossature. La liaison virtuelle doit être établie entre deux ABR ayant un domaine commun, avec un ABR connecté à l'ossature.

Authentification OSPF

Reportez-vous à MU-7.6.3 - Activation de l'authentification OSPF page 183 pour de plus amples informations sur l'authentification OSPF.

MU-7.6.2 Activation OSPF

L'OSPF n'a pas besoin d'être activé en tant que tel.

En modifiant les attributs de configuration sous les objets router/ospf et router/ospf/Area[ ] , l'OSPF peut être appliqué dans un système autonome. Reportez-vous à MR-1.10 - OSPF configuration attributes page 131.

L'objet router/ospf/Area[ ] n'est pas présent dans l'arborescence par défaut. Si vous souhaitez utiliser les fonctions associées à cet objet, vous devez d'abord ajouter cet objet. Reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43.

MU-7.6.3 Activation de l'authentification OSPF

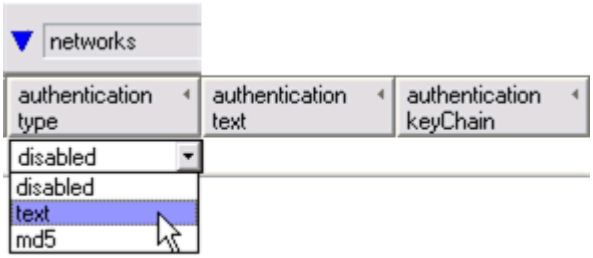
Il est possible d'authentifier les paquets OSPF afin que les routeurs puissent participer aux domaines d'acheminement en fonction des mots de passe prédéfinis. Par défaut, un routeur utilise une authentification Nulle qui signifie que les échanges par un réseau ne sont pas authentifiés. Il existe deux autres méthodes d'authentification: l'authentification par mot de passe simple et l'authentification Message Digest (MD-5):

Authentification	Description
Authentification Nulle	Aucune authentification n'est utilisée.
Authentification par mot de passe simple	Cela permet à un mot de passe (code) d'être configuré pour chaque interface. Les interfaces des différents routeurs qui souhaitent échanger des informations OSPF doivent être configurées avec le même code.
Authentification Message Digest (MD-5)	Il s'agit d'une authentification cryptographique. Un code (mot de passe) et une ID de code sont configurés sur chaque routeur. Le routeur utilise un algorithme basé sur le paquet OSPF, le code et l'ID de code pour générer un "prétraitement de message" qui est ajouté au paquet. Contrairement à ce qui se produit avec l'authentification simple, le code n'est pas échangé par le câble.

L'authentification OSPF peut être activée ou désactivée pour chaque interface.

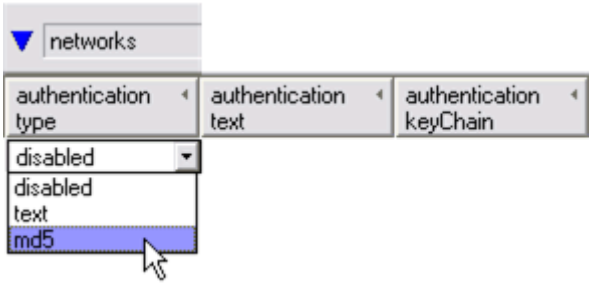
Activation de l'authentification par mot de passe simple

Pour activer l'authentification par mot de passe simple, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence, allez à l'objet router/ospf/Area[ ] et sélectionnez l'attribut de configuration networks Dans la structure authentication , réglez l'élément authentication type sur text. 
2	Dans l'élément authentication text, entrez le mot de passe.

Activation de l'authentification MD-5

Pour activer l'authentification MD-5, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence, allez à l'objet router/ospf et sélectionnez l'attribut de configuration keyChains Dans la table keyChains, ajoutez une nouvelle chaîne.
2	Dans la table chain, définissez correctement les éléments. Reportez-vous à telindus1421Router/router/ospf/keyChains/chain page 134.
3	Dans l'arborescence, allez à l'objet router/ospf/Area[ ] et sélectionnez l'attribut de configuration networks Dans la structure authentication , réglez l'élément authentication type sur md5.. 
4	Dans l'élément authentication keyChain, entrez le nom de la chaîne clé qui sera utilisée.

Dans les représentations d'écran ci-dessus, la structure authentication est expliquée comme faisant partie de la table networks. Notez que la structure authentication est également présente dans la table virtualLinks.

MU-7.7 Configuration de translation d'adresses

Cette section explique la translation d'adresse réseau (NAT) et la translation d'adresse port (PAT). Elle présente d'abord les deux concepts. Ensuite, une table vous permet de déterminer quelle méthode de translation répond le mieux à vos besoins. Enfin, cette section vous apprend comment configurer NAT et PAT.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.7.1 - Introduction à la translation d'adresses page 186
- MU-7.7.2 - Quand utiliser NAT et/ou PAT page 188
- MU-7.7.3 - Activation PAT sur une interface page 189
- MU-7.7.4 - Comment fonctionne la PAT? page 191
- MU-7.7.5 - Limitations PAT et solutions de rechange page 194
- MU-7.7.6 - Activation NAT sur une interface page 195
- MU-7.7.7 - Ajout de plusieurs objets NAT page 197
- MU-7.7.8 - Comment fonctionne la NAT? page 199
- MU-7.7.9 - Combinaison PAT et NAT page 201
- MU-7.7.10 - Easy NAT sur PPP page 201

MU-7.7.1 Introduction à la translation d'adresses

Qu'est-ce que la translation d'adresses?

La translation d'adresses est utilisée pour convertir des adresses IP privées en adresses IP officielles. Ce procédé est également connu sous le nom d'usurpation d'identité IP.

Pourquoi utiliser la translation d'adresses?

Chaque unité connectée à l'internet doit avoir une adresse IP *officielle* (c'est-à-dire unique). Le succès de l'internet a entraîné un manque d'adresses IP officielles. En conséquence, votre fournisseur d'accès (ISP) peut vous proposer une seule ou un petit nombre d'adresses IP officielles.

Si le nombre d'unités IP sur votre réseau local est supérieur au nombre d'adresses IP officielles, vous pouvez affecter des adresses IP de test ou *privées* à votre réseau local. Dans ce cas, vous devez configurer le routeur pour qu'il convertisse les adresses IP en utilisant NAT ou PAT.

Même s'il y a suffisamment d'adresses IP officielles disponibles, vous pouvez toujours choisir d'utiliser NAT p. ex. pour conserver des adresses de test préalablement affectées à toutes les unités de votre réseau local.

Qu'est-ce que le NAT?

Network Address Translation (NAT) est une norme internet qui permet à un réseau local (LAN) d'utiliser un ensemble d'adresses IP pour le trafic interne (adresses IP privées) et un autre ensemble d'adresses pour le trafic externe (adresses IP officielles). Le routeur d'accès (situé là où le LAN rencontre l'internet) procède à toutes les translations d'adresses IP nécessaires. C'est un processus dynamique.

Le NAT a trois fonctions principales:

- Il fournit une sortie de pare-feu en cachant les adresses IP internes.
- Il permet à une entreprise d'utiliser plus d'adresses IP internes. Puisqu'elles ne sont utilisées qu'en interne, il n'y a pas de possibilité de conflit avec des adresses IP utilisées par d'autres sociétés et organisations.
- Il permet à une société de combiner plusieurs connexions ISDN en une seule connexion internet.

Le nombre d'utilisateurs simultanés ayant un accès à l'internet est limité au nombre d'adresses IP officielles.

Qu'est-ce que le PAT?

Port Address Translation (PAT) est un type de translation d'adresses réseau (NAT). Avec le PAT, chaque ordinateur du LAN se voit affecter la même adresse IP, mais avec une affectation de numéro de port différente.

Seules les sessions TCP sortantes sont supportées.

Gamme d'adresses IP privées

L'autorité internationale de régulation, l'IANA, attribue les adresses IP officielles (appelées également globales). Elle a également défini trois gammes d'adresses IP à des fins d'usage privé. Cela signifie que vous pouvez utiliser ces adresses sans enregistrement sur votre réseau interne, tant que vous n'êtes pas connectés à l'internet.

Gamme d'adresses IP privées	Remarques
10.0.0.0 - 10.255.255.255	1 réseau de classe A
172.16.0.0 - 172.31.255.255	16 réseaux de classe B
192.168.0.0 - 192.168.255.255	256 réseaux de classe C

Vous pouvez définir des (sous-)réseaux dans ces gammes pour vos *adresses IP privées*.

MU-7.7.2 Quand utiliser NAT et/ou PAT

Reportez-vous à MU-7.7.1 - Introduction à la translation d'adresses page 186 pour une introduction à l'authentification NAT et PAT.

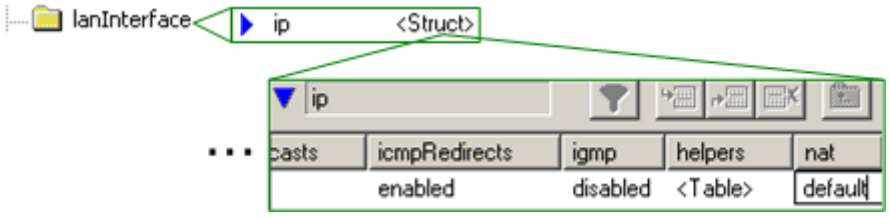
Vérifiez dans le tableau qui suit si vous avez besoin de NAT et/ou de PAT:

Nbre d'adresses IP officielles	**Nbre d'unités sur le réseau local**	**NAT ou PAT?**	**Reportez-vous au…**
1	plus de 1	Utilisez PAT.	MU-7.7.3 - Activation PAT sur une interface page 189
k (> 1)	plus de k	Utilisez NAT en combinaison avec PAT.	MU-7.7.9 - Combinaison PAT et NAT page 201
au moins k	k (≥ 1)	1. Aucune translation nécessaire. 2. Si vous souhaitez une translation, utilisez NAT.	1. Sautez cette section. 2. MU-7.7.6 - Activation NAT sur une interface page 195

MU-7.7.3 Activation PAT sur une interface

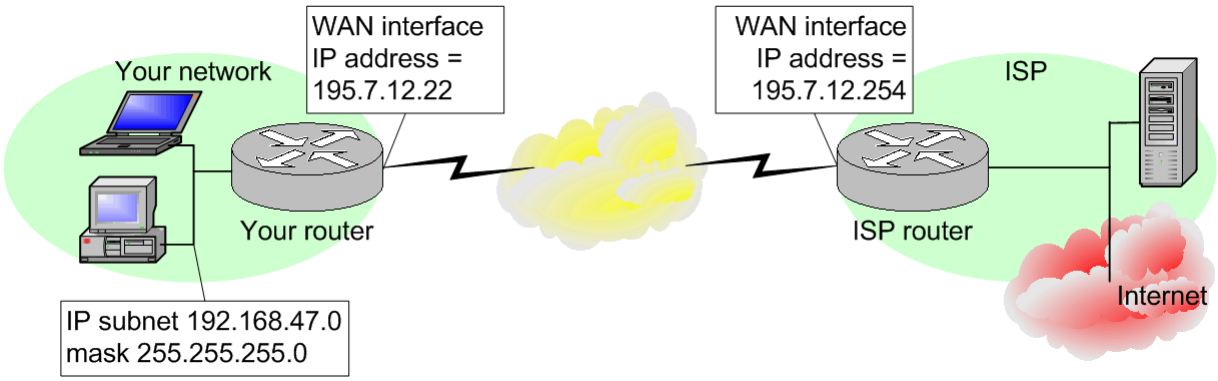
Reportez-vous à MU-7.7.1 - Introduction à la translation d'adresses page 186 pour une introduction au PAT.

Pour activer PAT sur une interface donnée, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router/defaultNat. Dans cet objet, configurez l'attribut patAddress. Utilisez cet attribut pour entrer l'adresse IP officielle qui doit être utilisée pour PAT. Entrer une adresse différente de la valeur par défaut 0.0.0.0 active automatiquement la PAT. Vous pouvez maintenant activer ou désactiver la PAT sur chaque interface IP. Notez que par défaut, PAT est activé sur toutes les interfaces IP.
2	Dans l'objet router/defaultNat, configurez l'attribut gateway. Utilisez cet attribut pour définir les adresses de passerelle provenant des trajets auxquels la PAT doit s'appliquer. Si vous ne configurez pas l'attribut gateway, l'attribut router/defaultRoute est alors pris comme adresses de passerelle uniquement.
3	Chaque interface IP a une structure ip. Utilisez les éléments suivants de la structure ip pour activer ou désactiver la PAT sur chaque interface IP: • nat. Utilisez cet élément pour activer la translation d'adresse sur l'interface. Pour ce faire, entre la chaîne “default“ comme valeur de l'élément nat. Se faisant, les réglages sont appliqués tels que définis dans l'objet router/defaultNat. Par exemple, les points qui suivent montrent l'emplacement de la structure ip sur l'interface LAN:  Reportez-vous à MU-5.2.2 - Où trouver les paramètres IP? page 54 pour l'emplacement de la structure ip sur les différentes interfaces IP.

Exemple – configuration de PAT

Supposons que votre réseau soit connecté par le réseau d'un opérateur à un fournisseur d'accès à l'internet (ISP). Vous avez reçu une seule adresse IP officielle de votre ISP, à savoir 195.7.12.22.



Les points qui suivent montrent comment activer la PAT:

- Dans l'objet router/defaultNat, réglez l'attribut patAddress sur 195.7.12.22. Dans ce cas, l'adresse PAT est la même que l'adresse IP qui est utilisée sur l'interface WAN.
- Dans l'objet router/defaultNat, réglez l'attribut gateway sur 195.7.12.254. Si, toutefois, vous avez déjà défini l'attribut router/defaultRoute sur 195.7.12.254, vous pouvez laisser l'attribut gateway vierge. Si l'attribut gateway est vierge, l'attribut defaultRoute est pris comme adresse de passerelle uniquement.
- Dans la structure ip de l'interface WAN, entrez la chaîne “default” comme valeur de l'élément nat.

MU-7.7.4 Comment fonctionne la PAT?

Prenons encore la topologie du réseau telle que décrite dans MU-7.7.3 - Activation PAT sur une interface page 189.

Les deux paragraphes qui suivent décrivent comment le Routeur Telindus 1421 SHDSL traite le trafic entrant et sortant lorsque la PAT est appliquée:

- Trafic sortant (vers l'internet) page 191.
- Trafic entrant (depuis l'internet) page 193.

Trafic sortant (vers l'internet)

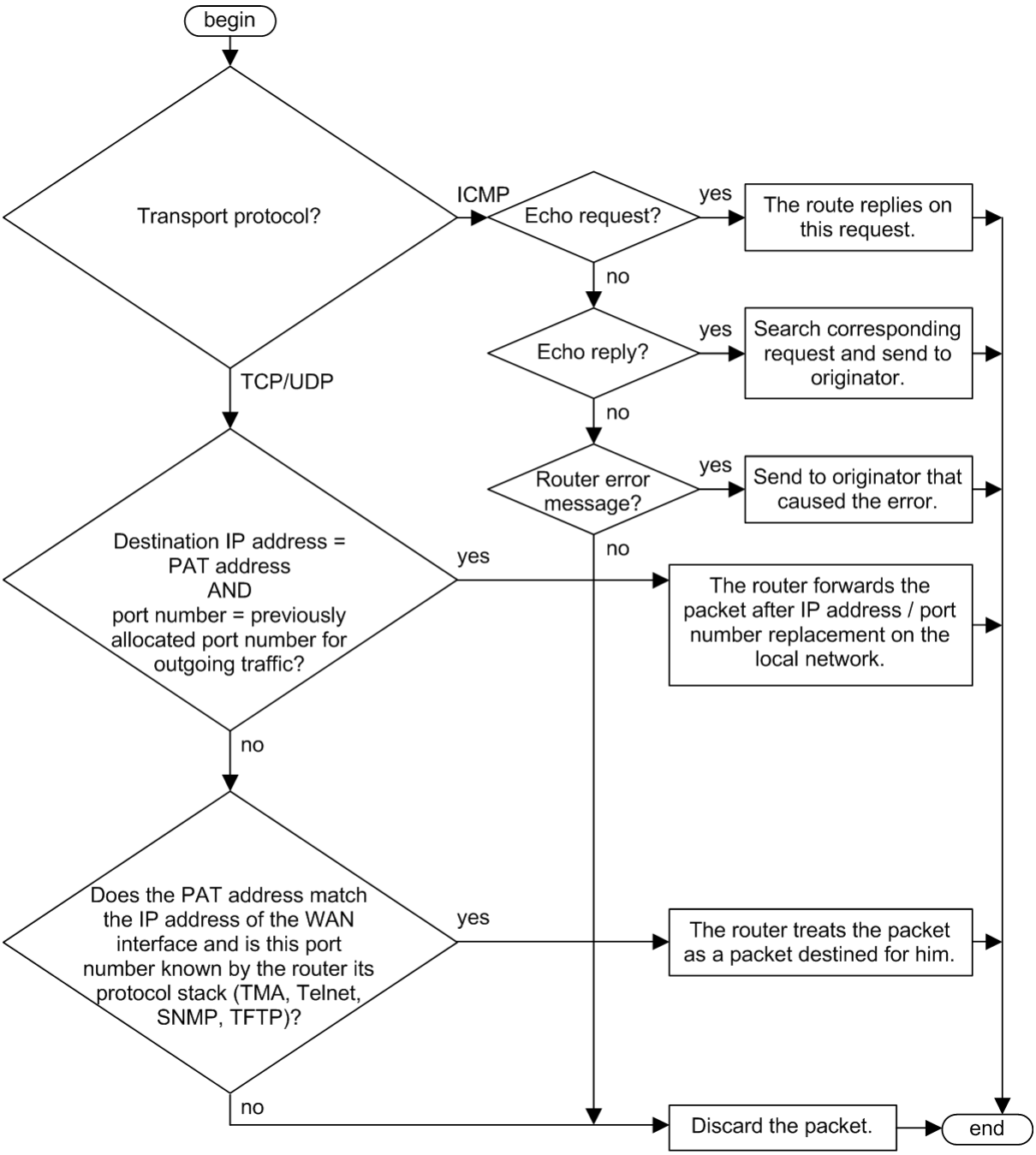
Le Routeur Telindus 1421 SHDSL remplace l'adresse source par son adresse PAT dans tout le trafic provenant du réseau local et destiné à l'internet. En fonction du protocole de transport IP et du nombre d'utilisateurs accédant simultanément à l'internet, le Routeur Telindus 1421 SHDSL envisage plusieurs actions:

Protocole		
TCP	**Description**	Il s'agit d'un protocole orienté selon la connexion: deux unités communiquant avec le protocole TCP constituent une session avant d'échanger les données utilisateur. Lorsqu'elles ont fini d'échanger les données utilisateur, la session est fermée. Des exemples de ce type d'application sont Telnet, HTTP et FTP. L'en-tête TCP contient un champ*port* indiquant le protocole de couche supérieure.
	Action	Lorsqu'une session débute, un numéro de port spécifique est affect à cette session. Tout le trafic provenant de cette session est affecté à ce numéro de port spécifique. Le numéro de port spécifique est libéré dans les 5 minutes qui suivent la fermeture de la session TCP (c'est-à-dire après un TCP Reset ou TCP Finish). Si la session n'a pas été correctement fermée, le numéro de port est libéré 24 heures après le dernier trafic de la session. Cette durée peut être configurée (reportez-vous à telindus1421Router/router/defaultNat/tcpSocketTimeOut page 101).
UDP	**Description**	Il s'agit d'un protocole sans connexion: les données utilisateurs peuvent être envoyées sans établir au préalable une session. Des exemples de ce type d'application sont SNMP et TFTP. Bien que TFTP soit orienté selon la session, il établit la session à un niveau supérieur et utilise UDP pour sa simplicité en tant que protocole de transport. L'en-tête UDP contient un champ*port* indiquant le protocole de couche supérieure.
	Action	Le numéro du port de source est remplacé par un numéro de port spécifique. Tout le trafic provenant de cette paire adresse IP / numéro de port source est affecté à ce numéro de port spécifique. S'il n'y a pas de trafic pendant 5 à 10 minutes, le numéro de port spécifique est libéré. Si la session n'a pas été correctement fermée, le numéro de port est libéré 3 minutes après le dernier trafic de session. Cette durée peut être configurée (reportez-vous à telindus1421Router/router/defaultNat/udpSocketTimeOut page 101).

Protocole		
ICMP	**Description**	Il s'agit d'un protocole sans connexion: les données utilisateurs peuvent être envoyées sans établir au préalable une session. Un exemple d'une telle application est l'utilitaire ping. Ces protocoles n'ont pas de numéros de port.
	Action	Chaque paquet ICMP est transmis vers l'internet. Chaque paquet ICMP est considéré comme une nouvelle session. S'il n'y a pas de trafic pendant 5 à 10 minutes, la session est fermée. Le fait qu'il soit possible d'ouvrir un total de 2048 sessions simultanées et que chaque paquet ICMP soit considéré comme une nouvelle session implique que, par exemple, une série continue de demandes ping à une vitesse d'une par seconde affecte entre 300 et 600 sessions.

Trafic entrant (depuis l'internet)

Supposons que le réseau IP WAN décrit dans MU-7.7.3 - Activation PAT sur une interface page 189 travaille en mode de numérotation[1]. Le trafic entrant depuis l'internet peut être destiné au réseau local, ou au routeur lui-même. Le routeur traite le trafic entrant sur l'adresse PAT de la façon suivante:


begin
Transport protocol?
ICMP
Echo request?
yes
The route replies on this request.
no
Echo reply?
yes
Search corresponding request and send to originator.
no
Router error message?
yes
Send to originator that caused the error.
no
TCP/UDP
Destination IP address = PAT address AND port number = previously allocated port number for outgoing traffic?
yes
The router forwards the packet after IP address / port number replacement on the local network.
no
Does the PAT address match the IP address of the WAN interface and is this port number known by the router its protocol stack (TMA, Telnet, SNMP, TFTP)?
yes
The router treats the packet as a packet destined for him.
no
Discard the packet.
end

1. Mode numéroté signifie que chaque interface WAN a une adresse IP. Dans ce cas, vous avez besoin de l'adresse IP officielle unique pour votre interface WAN.

MU-7.7.5 Limitations PAT et solutions de rechange

limitations PAT

La Port Address Translation a certaines limites:

- Certaines applications TCP ou UDP ne supportent pas la translation de port.
- Seules les sessions sortantes sont supportées. Ceci implique que vous ne pouvez accéder aux serveurs sur votre réseau local par le biais de l'internet.
- Support ICMP limité.

Solutions de rechange aux limites PAT

Utilisez les attributs suivants pour surmonter en partie les limitations PAT:

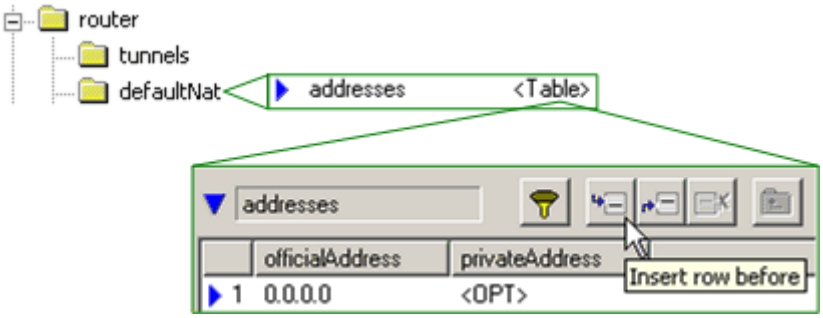
Attribut	Description
portTranslations	Vous pouvez trouver cet attribut dans l'objet router/defaultNat. Utilisez cet attribut pour définir les gammes de numéros de port spécifique qui ne doivent pas être converties lors de l'utilisation de la PAT. Reportez-vous à telindus1421Router/router/defaultNat/portTranslations page 99. **Exemple – configuration de la table portTranslations** TMA est un exemple d'application qui ne supporte pas la conversion de port. Si vous souhaitez assurer des connexions TMA de votre réseau local vers l'extérieur, vous devez indiquer le numéro de port TMA 1728 dans cette table. Toutefois, rappelez-vous que même alors, il n'est toujours pas possible d'avoir deux sessions TMA simultanées vers la même adresse extérieure. portTranslations protocol / startPort / endPort / action 1 udp 1728 <Opt> no translation 2 udp 2000 3000 deny Si vous ne souhaitez pas que les paquets UDP ayant des numéros de paquets compris entre 2000 et 3000 soient envoyés vers l'extérieur, vous devez également les inclure dans la table.
servicesAvailable	Vous pouvez trouver cet attribut dans l'objet router/defaultNat. Utilisez cet attribut pour définir les gammes de numéros de port spécifique pour le trafic internet entrant qui ne doivent pas être converties lors de l'utilisation de la PAT. Au lieu de cela, il est envoyé à l'adresse IP privée correspondante. Reportez-vous à telindus1421Router/router/defaultNat/servicesAvailable page 100. **Exemple – configuration de la table servicesAvailable** Dans cet exemple, un serveur web ayant l'adresse 192.168.47.250 sur le réseau local est accessible depuis l'internet bien qu'il n'ait pas d'adresse IP officielle. servicesAvailable protocol / startPort / endPort / serverAddress 1 tcp 80 <Opt> 192.168.47.250

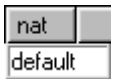
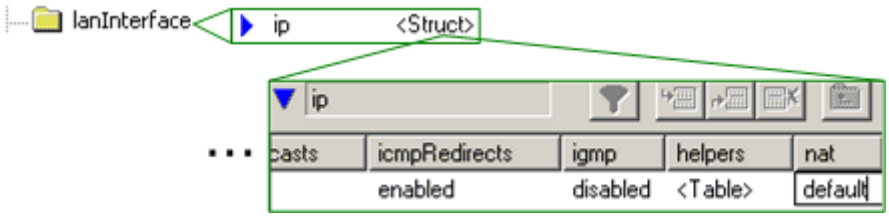
MU-7.7.6 Activation NAT sur une interface

Reportez-vous à MU-7.7.1 - Introduction à la translation d'adresses page 186 pour une introduction à la NAT.

En dépit des solutions de rechange proposées par les deux attributs de configuration PAT mentionnés ci-dessus pour surmonter les limitations de la PAT (reportez-vous à MU-7.7.5 - Limitations PAT et solutions de rechange page 194), il existe certaines situations où la PAT s'avère inadaptée. Par exemple, il n'est pas possible d'avoir plusieurs serveurs web sur votre réseau local. Il est également impossible de faire tourner une application avec des numéros de port de source fixe sur plusieurs unités locales connectées simultanément à une seule unité internet. Cela ne peut être résolu qu'en utilisant plusieurs adresses IP officielles: Network Address Translation.

Pour activer la NAT sur une interface donnée, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router/defaultNat ou ajoutez votre propre objet NAT sous l'objet router, p. ex. router/nat[myNat] (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43).
2	Dans l'objet NAT (par défaut ou initié par l'utilisateur), sélectionnez l'attribut addresses et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour entrer l'adresse IP officielle qui doit être utilisée pour NAT. Entrer une adresse dans la table addresses active automatiquement le processus NAT général. Vous pouvez maintenant activer ou désactiver la NAT sur chaque interface IP. Notez que par défaut, la NAT est activée sur toutes les interfaces IP.
3	Configurez les éléments du tableau addresses: • officialAddress. Utilisez cet élément pour définir l'adresse IP officielle. Ces adresses sont utilisées dans l'ordre inverse de leur apparition dans la liste. • privateAddress. Utilisez cet élément pour définir l'adresse IP privée, c'est-à-dire pour affecter en permanence une adresse IP officielle à une adresse privée.
4	Dans l'objet NAT (par défaut ou initié par l'utilisateur), configurez l'attribut gateway. Utilisez cet attribut pour définir les adresses de passerelle provenant des trajets auxquels la NAT doit s'appliquer. Si vous ne configurez pas l'attribut gateway, l'attribut router/defaultRoute est alors pris comme adresses de passerelle uniquement.

Etape	Action
5	Chaque interface IP a une structure ip. Utilisez les éléments suivants de la structure ip pour activer ou désactiver la NAT sur chaque interface IP: • nat. Utilisez cet élément pour activer la translation d'adresse sur l'interface. Pour ce faire, entrez le nom de l'objet NAT que vous souhaitez appliquer. - Si vous souhaitez appliquer les réglages NAT tels que définis dans l'objet router/defaultNat, entrez la chaîne “default“ comme valeur de l'élément nat.  - Si vous souhaitez appliquer les réglages NAT tels que définis dans un objet NAT que vous avez vous-mêmes ajouté (p. ex. router/nat[myNat]), entrez alors le nom d'indice de l'objet NAT (dans ce cas “myNat”) comme valeur de l'élément nat. Par exemple, les points qui suivent montrent l'emplacement de la structure ip sur l'interface LAN:  Reportez-vous à MU-5.2.2 - Où trouver les paramètres IP? page 54 pour l'emplacement de la structure ip sur les différentes interfaces IP.

Remarque importante – utilisation de la NAT sur l'interface LAN

Prenons la configuration suivante:

- telindus1421Router/lanInterface/ip/address = 195.7.12.22
- telindus1421Router/router/defaultNat/addresses = { officialAddress = 195.7.12.22; privateAddress = <opt> }
- telindus1421Router/wanInterface/ppp/ip/address = 2.2.2.2

Cela signifie que la NAT est utilisée sur l'interface LAN et que le routeur utilise l'adresse 195.7.12.22 comme adresse IP officielle.

Le problème qui se pose ici est que le routeur ne peut plus être géré via l'interface LAN à l'aide de l'outil de gestion (TMA, Telnet, etc.). Cela est dû au fait que le trajet NAT a la priorité sur le trajet LAN et que, parce qu'il s'agit d'une adresse NAT, le routeur n'accepte pas le trafic entrant sur l'adresse 195.7.12.22.

La solution consiste à ajouter l'adresse IP WAN à la table addresses comme adresse privée: telindus1421Router/router/addresses = { officialAddress = 195.7.12.22; privateAddress = 2.2.2.2 }. Dans ce cas, l'outil de gestion “service” fonctionne sur l'adresse IP WAN. Cela signifie toutefois que le WAN doit être actif.

MU-7.7.7 Ajout de plusieurs objets NAT

Il est possible d'ajouter plusieurs objets NAT (jusqu'à 5). Cela signifie que 5 interfaces au maximum peuvent utiliser un objet NAT dédié.

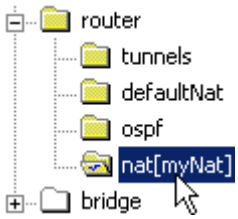
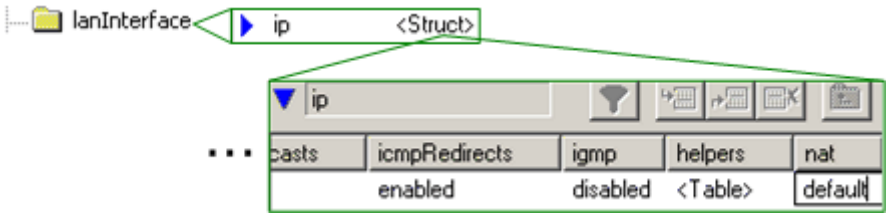
Deux ou plusieurs interfaces faisant référence à un seul et même objet NAT est une configuration non valable dont les résultats sont imprévisibles.

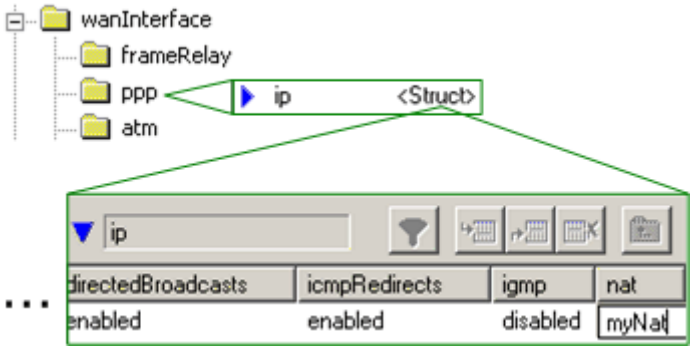
Exemple:

Supposons que sur un routeur Telindus 1421 SHDSL vous …

- souhaitiez ajouter 2 objets NAT: l'objet NAT par défaut (router/defaultNat) et un objet NAT initié par l'utilisateur (p. ex. router/nat[myNat]).
- souhaitiez appliquer l'objet NAT par défaut sur l'interface LAN et l'objet NAT initié par l'utilisateur sur l'interface WAN (et que l'interface WAN utilise, par exemple, PPP).

Procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Telindus 1421 SHDSL Router, allez à l'objet router/defaultNat et configurez les attributs de votre objet en fonction de vos besoins. Reportez-vous à MR-1.9.2 - NAT configuration attributes page 98.
2	Dans l'arborescence Telindus 1421 SHDSL Router, allez à l'objet router et ajoutez un objet nat en-dessous, p. ex. router/nat[myNat]. Reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43. 
3	Configurez les attributs dans l'objet router/nat[myNat] en fonction de vos besoins. Reportez-vous à MR-1.9.2 - NAT configuration attributes page 98.
4	Dans l'arborescence Telindus 1421 SHDSL Router tree, allez à l'objet lanInterface et sélectionnez la structure ip. Dans l'élément nat de la structure ip, entrez la chaîne “default”.  ⇒Les réglages NAT tels que définis dans l'objet router/defaultNat sont appliqués à l'interface LAN.

Etape	Action
5	Dans l'arborescence Telindus 1421 SHDSL Router, allez à l'objet wanInterface/ppp et sélectionnez la structure ip. Dans l'élément nat de la structure ip, entrez la chaîne “myNat”.  ⇒Les réglages NAT tels que définis dans l'objet router/nat[myNat] sont appliqués à l'interface WAN.

MU-7.7.8 Comment fonctionne la NAT?

Affectation dynamique d'une adresse IP officielle

Si une station locale envoie des données pour la première fois sur l'internet, la NAT recherche une adresse IP officielle non utilisée. Elle attribue cette adresse IP officielle à la station locale. Le nombre de stations locales pouvant accéder simultanément à l'internet est égal au nombre d'adresses NAT que vous avez définies. Si toutes les sessions entre une station locale et l'internet ont été fermées par l'application (en cas de TCP) ou par suite d'expirations de délais, l'ancienne IP officielle affectée au préalable est libérée pour une autre station locale.

Affectation statique d'une adresse IP officielle

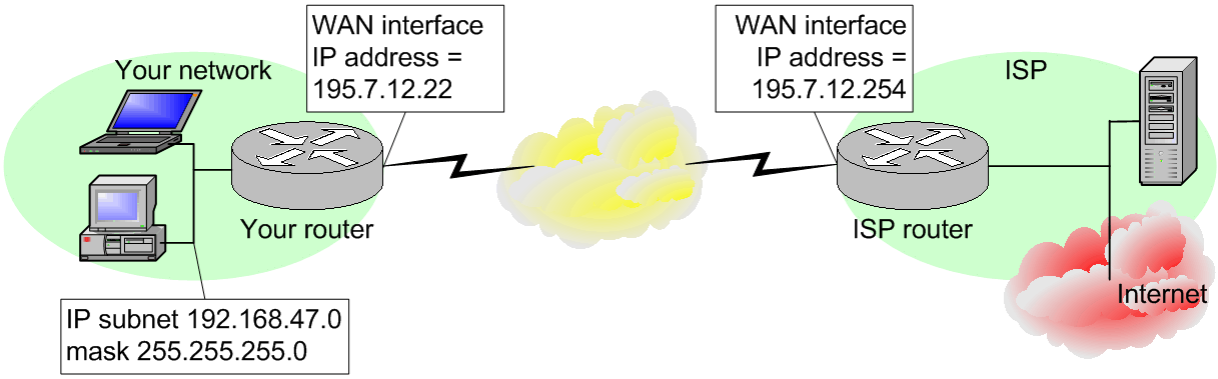
En option, l'entrée d'adresse NAT peut contenir une adresse IP privée correspondante. Cela permet d'affecter en permanence une adresse IP officielle à une station locale. Cela est utile pour les stations ou les serveurs qui doivent disposer en permanence d'un accès à l'internet. Un autre exemple d'adresses IP officielles affectées en permanence est un réseau où seul un nombre limité d'utilisateurs ont accès à l'internet.

Trafic entrant sur une adresse IP officielle

La NAT convertit uniquement les adresses IP et permet donc un trafic dans les deux sens. Toutefois, le trafic entrant sur les adresses IP officielles peut uniquement être transmis au réseau local si une adresse IP privée correspondante a été configurée.

Exemple – configuration de NAT

Supposons que votre réseau soit connecté par le réseau d'un opérateur à un fournisseur d'accès à l'internet (ISP). Vous avez reçu 4 adresses IP officielles de votre ISP, à savoir 195.7.12.21 à 195.7.12.24. Vous souhaitez attribuer l'une de ces adresses officielles en permanence à un serveur web ayant l'adresse privée 192.168.47.250. Toutes les autres adresses officielles doivent être affectées de manière dynamique.



Les points qui suivent montrent comment activer la NAT:

- Dans l'objet router/defaultNat, configurez l'attribut addresses de la manière suivante:

addresses

	officialAddress	privateAddress
1	195.7.12.21	192.168.47.250
2	195.7.12.22	<OPT>
3	195.7.12.23	<OPT>
4	195.7.12.24	<OPT>

- Dans l'objet router/defaultNat, réglez l'attribut gateway sur 195.7.12.254. Si, toutefois, vous avez déjà défini l'attribut router/defaultRoute sur 195.7.12.254, vous pouvez laisser l'attribut gateway vierge. Si l'attribut gateway est vierge, l'attribut defaultRoute est pris comme adresse de passerelle uniquement.
- Dans la structure ip de l'interface WAN, entrez la chaîne “default” comme valeur de l'élément nat.

MU-7.7.9 Combinaison PAT et NAT

Il est possible d'uti!liser une combinaison de PAT et de NAT. Dans ce cas, le routeur affecte d'abord des adresses NAT jusqu'à ce qu'elles soient toutes utilisées. Puis il utilise les adresses PAT pour la suite de la translation.

Assurez-vous que l'adresse PAT n'apparaît pas dans la table d'adresses NAT.

MU-7.7.10 Easy NAT sur PPP

qu'est-ce que Easy NAT sur PPP?

Easy NAT sur PPP signifie que dans une configuration typique client / ISP, la NAT est automatiquement activée sans qu'il soit besoin de la configurer spécifiquement.

Une configuration typique client / ISP est, par exemple, un routeur Telindus 1421 SHDSL côté client et un Telindus 2400 côté ISP connectés par une ligne SHDSL.

Quelles sont les conditions de Easy NAT sur PPP?

Les conditions de Easy NAT sur PPP sont:

- Une connexion A PPP (ou PPPoA) entre l'ISP et le client.
- Une interface PPP sur le routeur ISP:
  - le mode est acheminement.
  - Une adresse IP locale peut être configurée, ou peut provenir du LAN (non numéroté).
  - Une adresse IP distante est imposée au routeur du client.
  - La NAT est désactivée.
- Une interface PPP sur le routeur client:
  - le mode est acheminement.
  - Aucune adresse IP locale ou distante n'est configurée.
  - La NAT est activée (référence à l'objet defaultNat).
- L'objet defaultNat sur le routeur du client:
  - Aucune adresse PAT n'est configurée.
  - Aucune adresse NAT n'est configurée.

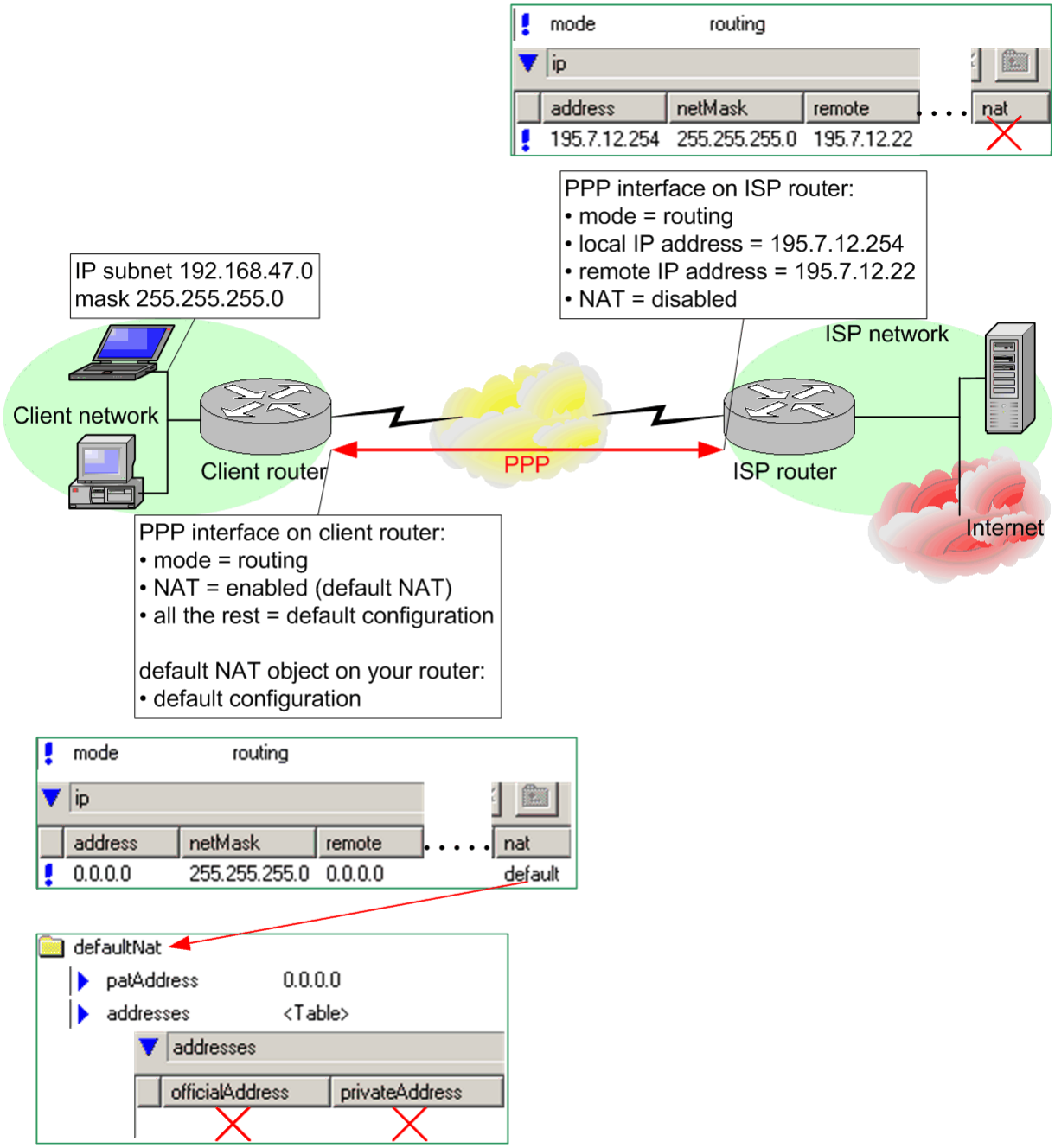
que fait Easy NAT sur PPP?

Une fois remplies les conditions énoncées ci-dessus, il se produit la chose suivante:

- Le routeur du client apprend l'adresse IP locale et distante de la liaison PPP à partir du routeur ISP.
- Le routeur du client ajoute un trajet vers le routeur ISP.
- Le routeur du client active la NAT sur l'interface PPP.

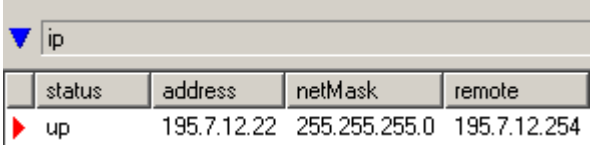
Exemple – Easy NAT

Supposons que vous ayez la configuration suivante:

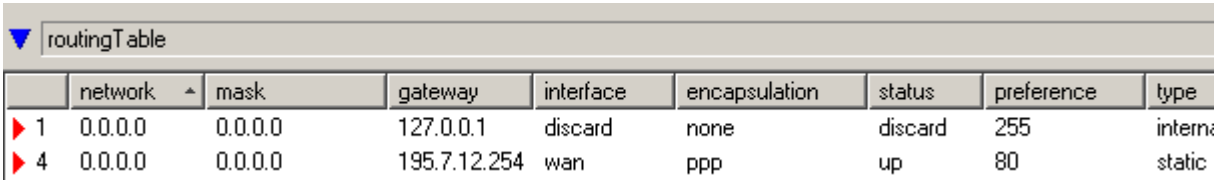


Une fois la liaison PPP active et opérationnelle, vous voyez que …

- le routeur du client apprend l'adresse IP locale et distante de la liaison PPP du routeur ISP. Vous pouvez le vérifier en observant l'état IP de la liaison PPP:



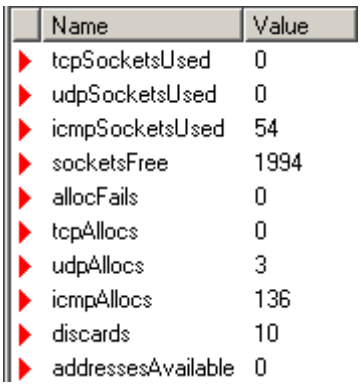
- Le routeur du client ajoute un trajet vers le routeur ISP. Vous pouvez le vérifier en observant l'état de la table d'acheminement:



routingTable

	network	mask	gateway	interface	encapsulation	status	preference	type
1	0.0.0.0	0.0.0.0	127.0.0.1	discard	none	discard	255	interna
4	0.0.0.0	0.0.0.0	195.7.12.254	wan	ppp	up	80	static

- Le routeur du client active la NAT sur l'interface PPP. Vous pouvez le vérifier en observant les performances de la NAT. Lorsqu'une connexion avec l'ISP est active, vous voyez que l'attribut socketsFree diminue tandis que les fiches utilisées (xxxSocketsUsed) et les attributs d'affectation (xxxAllocs) augmentent.



Name	Value
tcpSocketsUsed	0
udpSocketsUsed	0
icmpSocketsUsed	54
socketsFree	1994
allocFails	0
tcpAllocs	0
udpAllocs	3
icmpAllocs	136
discards	10
addressesAvailable	0

MU-7.8 Configuration de la politique de trafic et de priorité sur le routeur

Cette section présente la politique de trafic et de priorité et donne une rapide description des attributs que vous pouvez utiliser pour configurer ces fonctions sur le routeur. Elle vous montre également la différence avec la politique de trafic sur le pont.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-7.8.1 - Présentation de la politique de trafic et de priorité page 205
- MU-7.8.2 - Politique de trafic et de priorité sur les données acheminées et pontées page 208
- MU-7.8.3 - Comment configurer une politique de trafic et de priorité sur le routeur? page 209
- MU-7.8.4 - Création d'une politique de trafic sur le routeur page 210
- MU-7.8.5 - Application d'une politique de trafic sur une interface du routeur page 212
- MU-7.8.6 - Création d'une politique de priorité page 213
- MU-7.8.7 - Application d'une politique de priorité sur une interface page 215
- MU-7.8.8 - Configuration de la politique de trafic et de priorité sur le routeur – un exemple page 216
- MU-7.8.9 - Attribut de la file par défaut ou profil de politique de trafic page 219

MU-7.8.1 Présentation de la politique de trafic et de priorité

Qu'est-ce que la politique de trafic et de priorité?

Du fait de la nature hasardeuse du trafic vocal / vidéo / de données, la quantité de trafic dépasse parfois la vitesse d'une liaison. A ce stade, le Routeur Telindus 1421 SHDSL doit décider que faire de cet “excédent” de trafic:

- Mettre le trafic dans une file d'attente et laisser passer le premier paquet de la file?
- Ou placer les paquets dans différentes files d'attente et s'occuper ce certaines files plus souvent que d'autres (mise en file d'attente prioritaire)?

Ces questions sont traitées par les mécanismes de politique de priorité et de trafic:

- La politique de trafic détermine, en condition de surcharge de trafic, comment et quelles files sont remplies par les données “en surplus”.
- La politique de priorité détermine comment et quelles files sont vidées.

Qu'est-ce que la mise en file d'attente prioritaire?

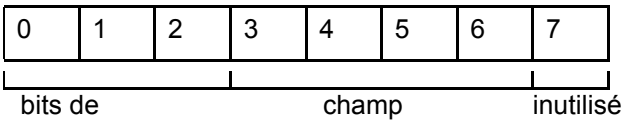
En utilisant les fonctions de la politique de trafic et de priorité, vous pouvez procéder à la mise en file d'attente prioritaire. Cela vous permet de définir comment prioritiser le trafic dans le réseau, par exemple pour garantir que la voix, la vidéo ou un autre support est traité avant (ou après) d'autres types de trafic, pour veiller à ce que le trafic de réponse du web est acheminé avant le trafic de navigation normal sur le web, etc.

Pour chaque interface (physique et logique), il existe 7 files:

File	Type de file	Description
1 - 5	file configurable par l'utilisateur	L'utilisateur peut décider quelles données vont dans quelle file.
6	file à faible temporisation	L'utilisateur peut décider quelles données vont dans cette file. Cette file est habituellement traitée plus souvent que les files configurables par l'utilisateur.
7	file système	Cette file est remplie par les données critiques de mission (p. ex. messages de contrôle de liaison, etc.) et a la priorité sur toutes les autres files.

Qu'est-ce que l'octet TOS?

L'octet Type Of Service (TOS) est un champ de 8 bits dans l'en-tête IP. Il est structuré de la façon suivante:



Qu'est-ce que le champ de précédence?

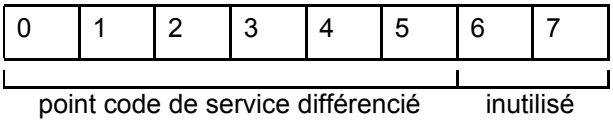
Le champ de précédence est un champ à trois bits dans l'octet TOS de l'en-tête IP (voir RFC 791). Ce champ permet à un administrateur réseau d'affecter des valeurs de 0 à 7 pour classifier et prioritiser les types de trafic. La précédence IP a tendance à être supprimée au bénéfice de DSCP, mais elle est supportée par de nombreuses applications et de nombreux routeurs.

Qu'est-ce que le champ TOS?

Le champ TOS est un champ à quatre bits dans l'octet TOS de l'en-tête IP (voir RFC 1349). Il permet d'affecter des valeurs comprises entre 0 et 15 pour des gestions spécifiques du trafic (par exemple, minimiser la temporisation, optimiser le débit). Le champ TOS est supprimé au bénéfice de DSCP.

Qu'est-ce que DSCP ou Diff-Serv?

Le Differentiated Services Code Point (DSCP) utilise l'octet TOS différemment (voir RFC 2474). Six bits de l'octet TOS sont réaffectés pour une utilisation comme champ DSCP, où chaque DSCP spécifie un comportement par saut particulier qui est appliqué à un paquet.



DSCP n'est pas compatible avec la précédence IP.

Qu'est-ce que PHB?

Un comportement par saut (Per-Hop Behaviour - PHB) est un mécanisme d'affectation de ressource par saut. Le PHB doit être considéré comme un comportement de transmission particulier qui s'étend sur un réseau et assure une certaine classe de service.

Le Routeur Telindus 1421 SHDSL propose le Assured Forwarding PHB (RFC 2597).

Qu'est-ce que AF PHB?

Assured Forwarding Per-Hop Behaviour (AF PHB, voir RFC 2597) définit une méthode de définition de la précédence de rejet. Les paquets IP sont repérés par une valeur de précédence de rejet parmi trois possibles. En cas de congestion, le nœud DS congestionné protège les paquets par une valeur de précédence de rejet inférieure en rejetant les paquets présentant une valeur de précédence de rejet plus élevée.

Qu'est-ce que l'IEEE 802.1P?

La technique de signalisation IEEE 802.1P (désignée souvent comme Class Of Service, COS) est une spécification IEEE de prioritisation du trafic du réseau sur la sous-couche liaison de données/MAC (couche 2).

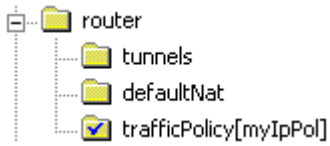
802.1P est un dérivé de la norme 802.1Q (tagging VLAN) et elles fonctionnent en tandem. La norme 802.1Q spécifie un tag qui se modifie en trame MAC. Le repère VLAN transporte les informations VLAN. Le repère VLAN se compose de deux parties: le VLAN ID (12 bits) et la prioritisation (3 bits). Le champ de prioritisation n'a jamais été défini dans la norme VLAN. La mise en œuvre 802.1P définit ce champ de prioritisation.

MU-7.8.2 Politique de trafic et de priorité sur les données acheminées et pontées

Reportez-vous à MU-7.8.1 - Présentation de la politique de trafic et de priorité page 205 pour la présentation.

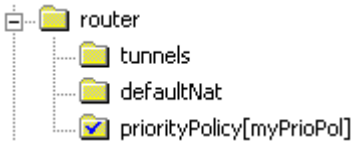
Politique de trafic sur les données acheminées et pontées

La politique de trafic (c'est-à-dire la politique de remplissage des files) n'est pas la même pour les données acheminées et pour les données pontées. Le tableau qui suit l'explique:

Si … est activé,	alors …
acheminement uniquement	Les données acheminées sont mises en file d'attente en utilisant les réglages de la politique de trafic telle que configurée dans l'objet trafficPolicy[ ] sous l'objet router.  Reportez-vous à MU-7.8.4 - Création d'une politique de trafic sur le routeur page 210.
pontage uniquement	Les données pontées sont mises en file d'attente en utilisant les réglages de la politique de trafic telle que configurée dans l'objet trafficPolicy[ ] sous l'objet bridge. Reportez-vous à MU-8.3.2 - Configuration d'une politique de trafic sur le pont page 249.
acheminement et pontage	• Les données acheminées sont mises en file d'attente en utilisant les réglages de politique de trafic telle que configurée dans l'objet trafficPolicy[ ] sous l'objet router. Reportez-vous à MU-7.8.4 - Création d'une politique de trafic sur le routeur page 210. • Les données pontées sont mises en file d'attente en utilisant les réglages de la politique de trafic telle que configurée dans l'objet trafficPolicy[ ] sous l'objet bridge Reportez-vous à MU-8.3.2 - Configuration d'une politique de trafic sur le pont page 249.

Politique de trafic sur les données acheminées et pontées

La politique de priorité (c'est-à-dire la politique de vidage des files) est la même pour les données acheminées et pontées. Les files sont vidées en utilisant les réglages de politique de priorité telle que configurée dans l'objet priorityPolicy[ ] sous l'objet router.



Reportez-vous à MU-7.8.6 - Création d'une politique de priorité page 213.

MU-7.8.3 Comment configurer une politique de trafic et de priorité sur le routeur?

Reportez-vous à MU-7.8.1 - Présentation de la politique de trafic et de priorité page 205 pour la présentation.

Pour configurer une politique de trafic et de priorité des données acheminées sur une interface donnée, procédez de la façon suivante:

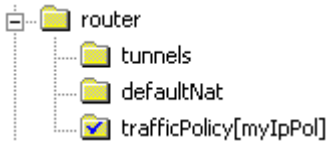
Etape	Action
1	Créez et configurez une politique de trafic d'acheminement. Reportez-vous à MU-7.8.4 - Création d'une politique de trafic sur le routeur page 210.
2	Appliquez la politique de trafic d'acheminement à l'interface souhaitée. Reportez-vous à MU-7.8.5 - Application d'une politique de trafic sur une interface du routeur page 212.
3	Créez et configurez une politique de priorité. Reportez-vous à MU-7.8.6 - Création d'une politique de priorité page 213.
4	Appliquez la politique de priorité à l'interface souhaitée. Reportez-vous à MU-7.8.7 - Application d'une politique de priorité sur une interface page 215.

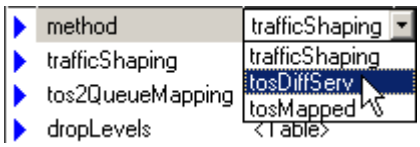
MU-7.8.4 Création d'une politique de trafic sur le routeur

Reportez-vous à MU-7.8.3 - Comment configurer une politique de trafic et de priorité sur le routeur? page 209 pour un aperçu de la manière de configurer une politique de trafic et de priorité. Pour vous permettre de suivre le processus, les points suivants vous en donnent un rapide aperçu.

- → **Créez et configurez une politique de trafic d'acheminement.** ← **Vous êtes ici.**
- Appliquez la politique de trafic d'acheminement à l'interface souhaitée.
- Créez et configurez une politique de priorité.
- Appliquez la politique de priorité à l'interface souhaitée.

Pour créer et configurer une politique de trafic des données acheminées sur une interface donnée, procédez de la façon suivante:

<table>
<tr><th>Etape</th><th>Action</th></tr>
<tr><td>1</td><td>Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et ajoutez un objet trafficPolicy[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43).
 

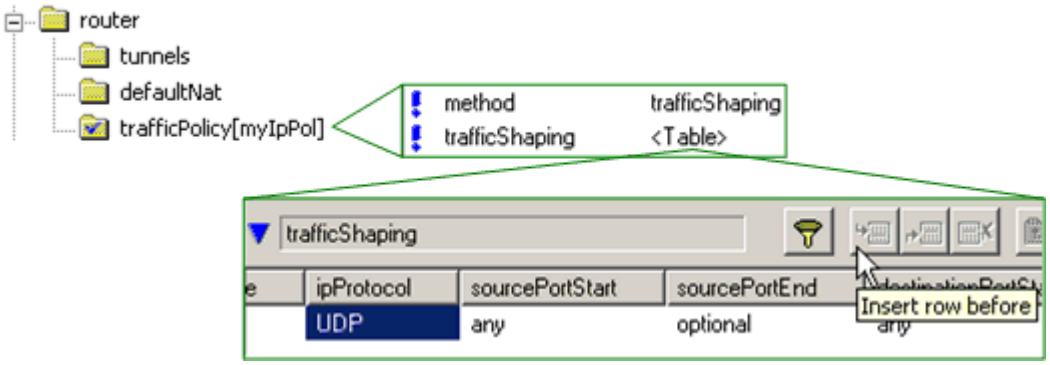
p. ex. trafficPolicy[myIpPol]</td></tr>
<tr><td>2</td><td>Dans l'objet trafficPolicy[ ] que vous venez d'ajouter, allez à l'attribut method. Utilisez cet attribut pour choisir une méthode de politique de trafic. La politique de trafic est alors utilisée pour déterminer, en condition de surcharge de trafic, comment et quelles files sont remplies par les données “en surplus”.
 

Reportez-vous à telindus1421Router/router/trafficPolicy[ ]/method page 117 pour de plus amples informations.</td></tr>
<tr><td>3</td><td>En fonction de la méthode de politique de trafic que vous avez sélectionnée, vous devez maintenant configurer les critères de politique:
<table>
<tr><th>Si vous choisissez la méthode …</th><th>utilisez ensuite l'attribut suivant pour configurer les critères de politique:</th></tr>
<tr><td>trafficShaping,</td><td>• trafficShaping.
• dropLevels (uniquement l'élément dropLevel1).</td></tr>
<tr><td>tosDiffServ,</td><td>dropLevels.</td></tr>
<tr><td>tosMapped,</td><td>• tos2QueueMapping.
• dropLevels (uniquement l'élément dropLevel1).</td></tr>
</table>
Pour de plus amples informations, se reporter à …
• telindus1421Router/router/trafficPolicy[ ]/trafficShaping page 119.
• telindus1421Router/router/trafficPolicy[ ]/dropLevels page 122.
• telindus1421Router/router/trafficPolicy[ ]/tos2QueueMapping page 124.</td></tr>
</table>

Exemple - création d'une politique de trafic sur le routeur

Supposons que vous créiez une politique de trafic qui utilise la méthode de configuration de trafic pour remplir les files d'attente, en conditions de surcharge de trafic, avec les données “en excédent”. Supposons que vous vouliez le faire uniquement pour le protocole UDP.

La figure qui suit vous montre comment procéder à la configuration:



MU-7.8.5 Application d'une politique de trafic sur une interface du routeur

Reportez-vous à MU-7.8.3 - Comment configurer une politique de trafic et de priorité sur le routeur? page 209 pour un aperçu de la manière de configurer une politique de trafic et de priorité. Pour vous permettre de suivre le processus, les points suivants vous en donnent un rapide aperçu.

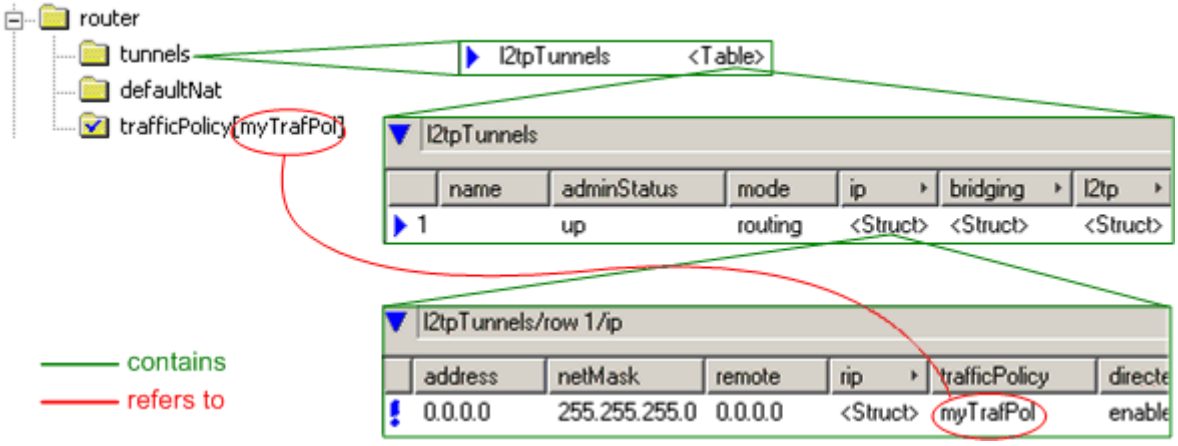
- Créez et configurez une politique de trafic d'acheminement.
- → **Appliquez la politique de trafic d'acheminement sur l'interface souhaitée.** ← **Vous êtes ici.**
- Créez et configurez une politique de priorité.
- Appliquez la politique de priorité à l'interface souhaitée.

Pour appliquer une politique de trafic aux données acheminées sur une interface donnée, entrez le nom d'indice de l'objet trafficPolicy[ ] crée auparavant comme valeur de l'élément trafficPolicy. L'élément trafficPolicy se trouve dans la structure ip de l'interface IP. Reportez-vous à MU-5.2.2 - Où trouver les paramètres IP? page 54 pour l'emplacement de la structure ip sur les différentes interfaces IP.

Exemple – application d'une politique de trafic sur une interface du routeur

Supposons que vous ayez créé et configuré un objet de politique de trafic avec le nom d'indice myTrafPol (c'est-à-dire trafficPolicy[myTrafPol]), et que vous souhaitiez appliquer cette politique de trafic à un tunnel L2TP créé auparavant.

La figure qui suit vous montre comment procéder à la configuration:



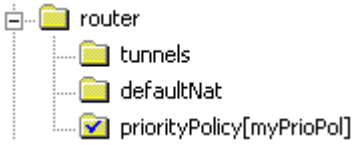
MU-7.8.6 Création d'une politique de priorité

Alors que la configuration d'une politique de trafic pour les données acheminées est différente de celle applicable aux données pontées, la configuration d'une politique de priorité est la même pour les deux. En d'autres termes, le mécanisme de remplissage des files d'attente est différent pour les données acheminées et pour les données pontées, mais le mécanisme de vidage des files est le même pour les deux.

Reportez-vous à MU-7.8.3 - Comment configurer une politique de trafic et de priorité sur le routeur? page 209 pour un aperçu de la manière de configurer une politique de trafic et de priorité. Pour vous permettre de suivre le processus, les points suivants vous en donnent un rapide aperçu.

- Créez et configurez une politique de trafic.
- Appliquez la politique de trafic à l'interface souhaitée.
- → **Créez et configurez une politique de priorité.** ← **Vous êtes ici.**
- Appliquez la politique de priorité à l'interface souhaitée.

Pour créer et configurer une politique de priorité pour une interface donnée, procédez de la façon suivante:

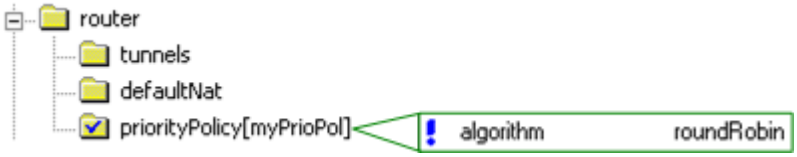
Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et ajoutez un objet priorityPolicy[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43). P. ex. trafficPolicy[myBridgePol] 
2	Dans l'objet priorityPolicy[ ] que vous venez d'ajouter, allez à l'attribut algorithm. Utilisez cet attribut pour déterminer comment et quelles files sont vidées. Reportez-vous à telindus1421Router/router/priorityPolicy[ ]/algorithm page 126 pour de plus amples informations.

Etape	Action
3	Configurez les autres attributs dans l'objet priorityPolicy[ ]. Les plus importants sont: • queueConfigurations. Utilisez cet attribut pour … - définir le nombre d'octets /paquets soris de la file configurable par l'utilisateur lorsque la file d'attente est traitée. - définir l'importance relative des files configurables par l'utilisateur. Reportez-vous à telindus1421Router/router/priorityPolicy[ ]/queueConfigurations page 129 pour de plus amples informations. • lowDelayQuotum. Utilisez cet attribut pour définir le nombre d'octets / paquets sortis de la file d'attente à faible temporisation lorsque celle-ci est traitée. Reportez-vous à telindus1421Router/router/priorityPolicy[ ]/lowdelayQuotum page 129 pour de plus amples informations. • largeur de bande. Utilisez cet attribut pour définir le Committed Information Rate (CIR) pour chaque file. Reportez-vous à telindus1421Router/router/priorityPolicy[ ]/bandwidth page 130 pour de plus amples informations.

Exemple - création d'une politique de trafic sur le routeur

Supposons que vous souhaitiez créer une politique de priorité qui utilise l'algorithme round-robin (chaîne d'événements survenant en séquences périodiques) pour vider les files.

La figure qui suit vous montre comment procéder à la configuration:



MU-7.8.7 Application d'une politique de priorité sur une interface

Reportez-vous à MU-7.8.3 - Comment configurer une politique de trafic et de priorité sur le routeur? page 209 pour un aperçu de la manière de configurer une politique de trafic et de priorité. Pour vous permettre de suivre le processus, les points suivants vous en donnent un rapide aperçu.

- Créez et configurez une politique de trafic.
- Appliquez la politique de trafic à l'interface souhaitée.
- Créez et configurez une politique de priorité.
- → **Appliquez la politique de priorité sur l'interface souhaitée.** ← **Vous êtes ici.**

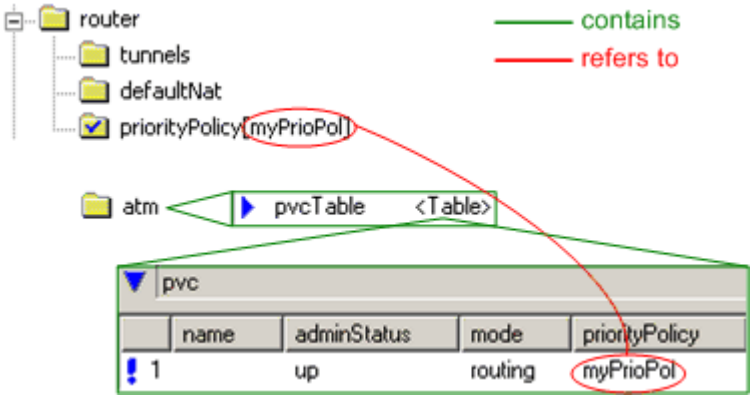
Pour appliquer une politique de priorité sur une interface donnée, entrez le nom d'indice de l'objet trafficPolicy[ ] crée auparavant comme valeur de l'élément trafficPolicy. L'attribut priorityPolicy se trouve dans …

- telindus1421Router/lanInterface/priorityPolicy. Dans ce cas, spécifiez une politique de priorité pour l'interface LAN.
- telindus1421Router/wanInterface/priorityPolicy. Dans ce cas, spécifiez une politique de priorité pour l'interface WAN complète (c'est-à-dire également pour toutes les interfaces logiques présentes sur l'interface WAN, comme ATM PVC, etc.).
- telindus1421Router/wanInterface/atm/pvcTable/priorityPolicy. Dans ce cas, spécifiez une politique de priorité pour chaque ATM PVC.
- telindus1421Router/wanInterface/frameRelay/dlciTable/priorityPolicy. Dans ce cas, spécifiez une politique de priorité pour chaque DLCI à Frame Relay.

Exemple - application d'une politique de priorité sur une interface

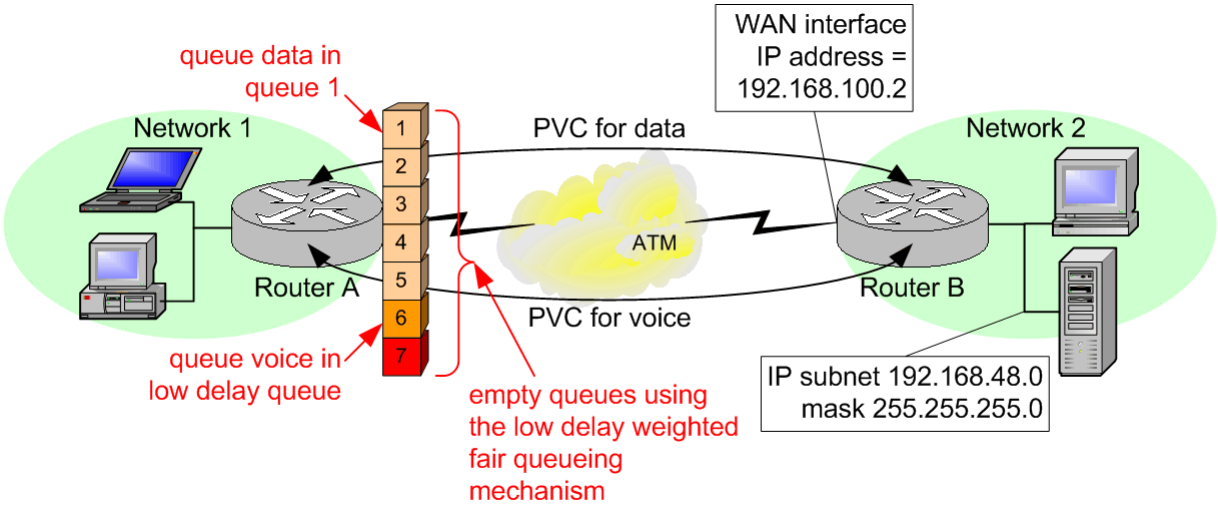
Supposons que vous ayez créé et configuré un objet de politique de trafic avec le nom d'indice myPrioPol (c'est-à-dire priorityPolicy[myPrioPol]), et que vous souhaitiez appliquer cette politique de trafic à un profil ATM PVC créé auparavant.

La figure qui suit vous montre comment procéder à la configuration:



MU-7.8.8 Configuration de la politique de trafic et de priorité sur le routeur – un exemple

Supposons que vous disposiez de deux réseaux interconnectés par un réseau ATM. Le réseau 1 transporte un mélange de trafic de données et de trafic vocal. Le trafic présent sur ce réseau est différencié en réglant les valeurs Type Of Service (TOS) dans les en-têtes de paquets IP (données = 0, voix = 10). Lorsque le trafic est acheminé du réseau 1 au réseau 2, vous voulez que le trafic de données et le trafic vocal passent chacun par une PVC distincte. De plus, en cas de congestion, vous voulez que la voix soit mise en file d'attente dans la file à faible temporisation et que les données soient mises dans la file 1. L'algorithme que vous voulez utiliser pour vider les files est le mécanisme de mise en attente à faible temporisation pondéré.

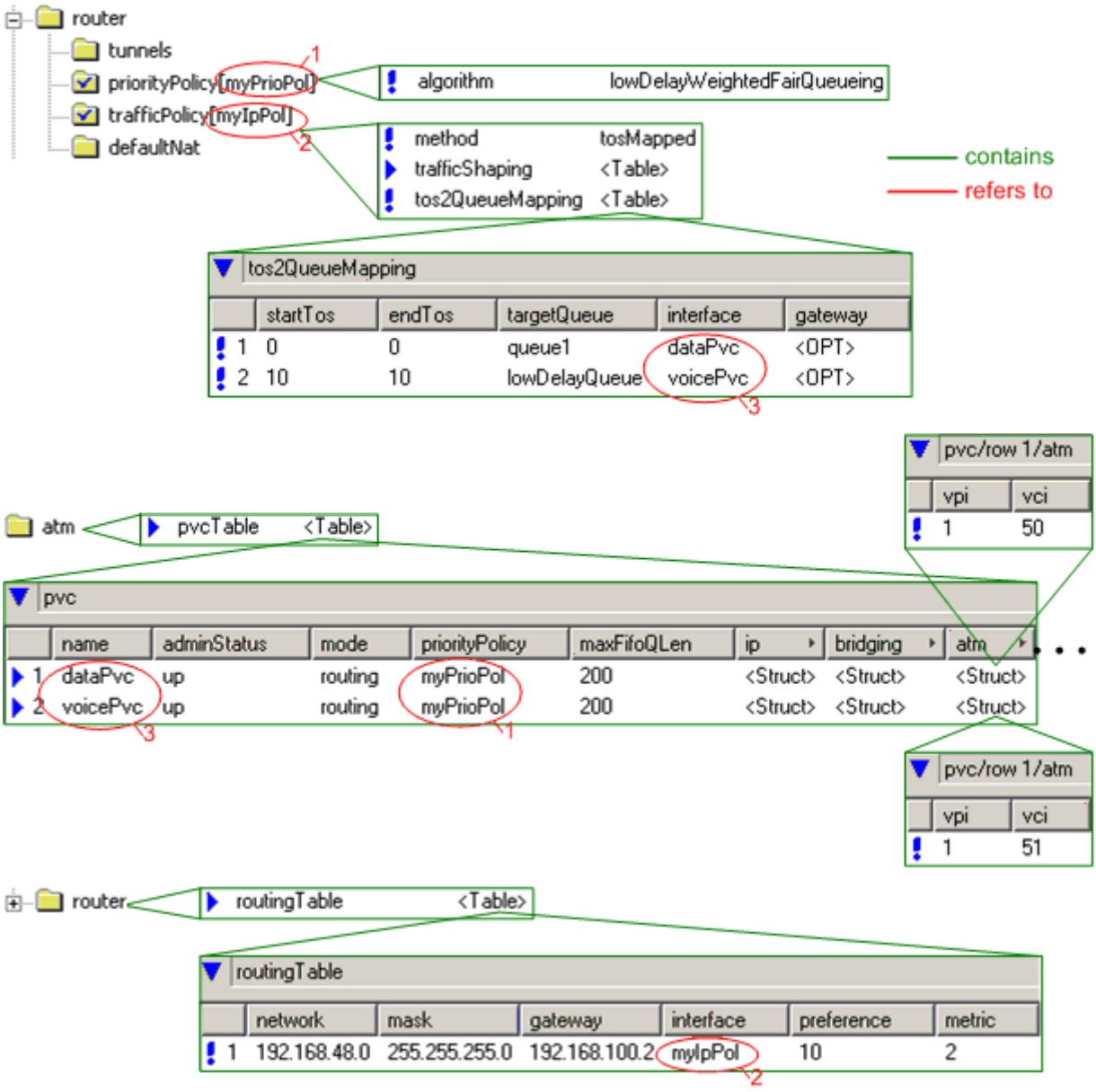


A grands traits, voici comment configurer cette disposition:

Etape	Action
1	Configurez deux PVC ATM. Par exemple: • Configurez une PVC ATM qui transportera le trafic de données, p. ex. pvc/name = dataPvc. • Configurez une autre PVC ATM qui transportera le trafic vocal, p. ex. pvc/name = voicePvc. Puisque ce n'est pas le sujet principal de cet exemple, reportez-vous, pour de plus amples informations sur la création de PVC ATM, à MU-6.2.2 - Configuration d'ATM PVC page 91.

Etape	Action
2	Créez et configurez une politique de trafic IP à des fins d'acheminement et de mise en file d'attente en fonction de la politique. Par exemple: • Créez un objet trafficPolicy[myIpPol]. • Réglez l'attribut method sur tosMapped. • Dans la table tos2QueueMapping, créez deux entrées et définissez les éléments startTos, endToset interface de chaque entrée de telle manière que le trafic de données et le trafic vocal passent chacun par une PVC distincte. Définissez également targetQueue pour les deux types de trafic: - la file à faible temporisation pour la voix. - la file 1 pour les données.
3	Créez un trajet qui “pointe” cette politique de trafic. Par exemple: Créez une entrée dans l'attribut routingTable dans lequel vous spécifiez que le trafic destiné au réseau 192.168.48.0 doit être envoyé selon la politique de trafic IP créée antérieurement.

La figure qui suit montre comment configurer la politique de trafic et de priorité que vous souhaitez:



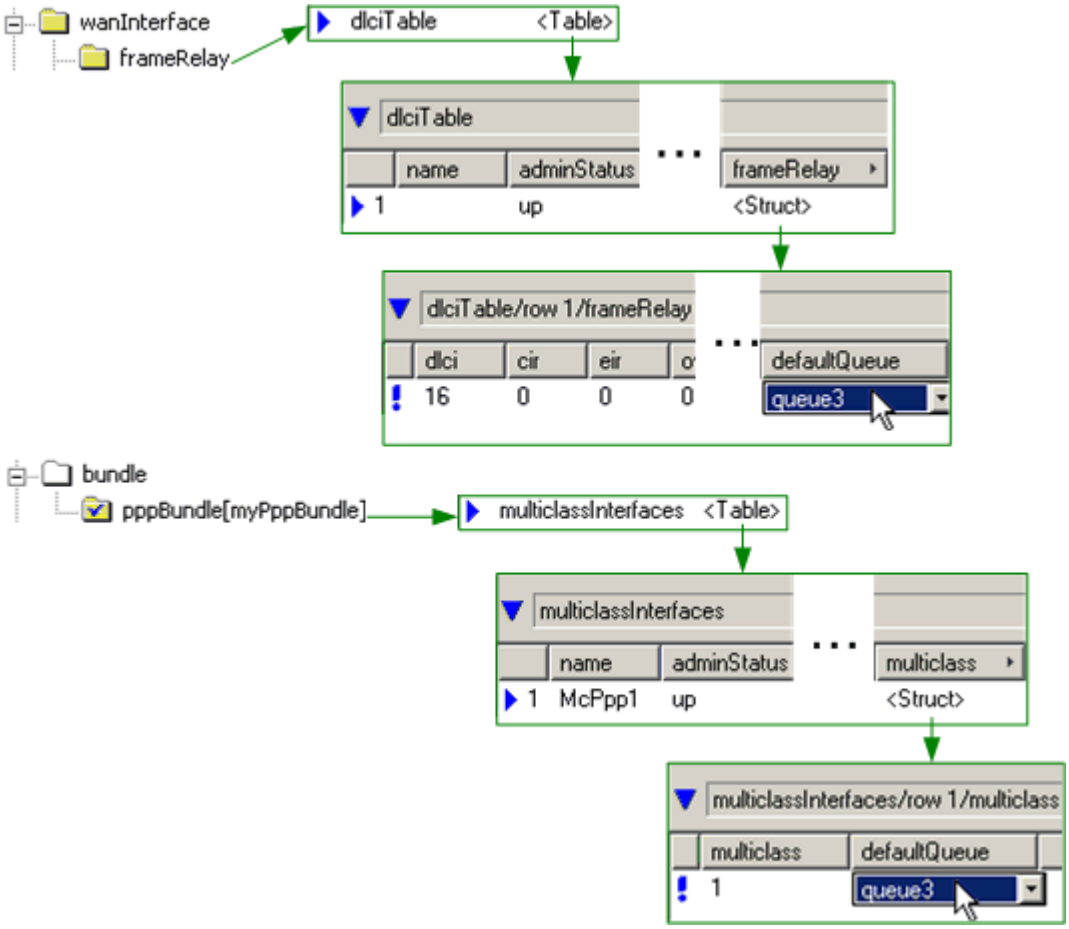
MU-7.8.9 Attribut de la file par défaut ou profil de politique de trafic

En cas de DLCI à Frame Relay et de liaisons PPP multiclasses, il est possible d'affecter une file par défaut à la liaison. Cela vous permet de configurer facilement une politique de trafic sans avoir à créer et à appliquer un profil de politique de trafic. Comme la plupart des configurations qui nécessitent le QoS partagent uniquement les flux vocaux et de données (souvent sur la base des adresses IP seulement), une telle configuration est plus directe.

Pour configurer une file par défaut, procédez de la façon suivante:

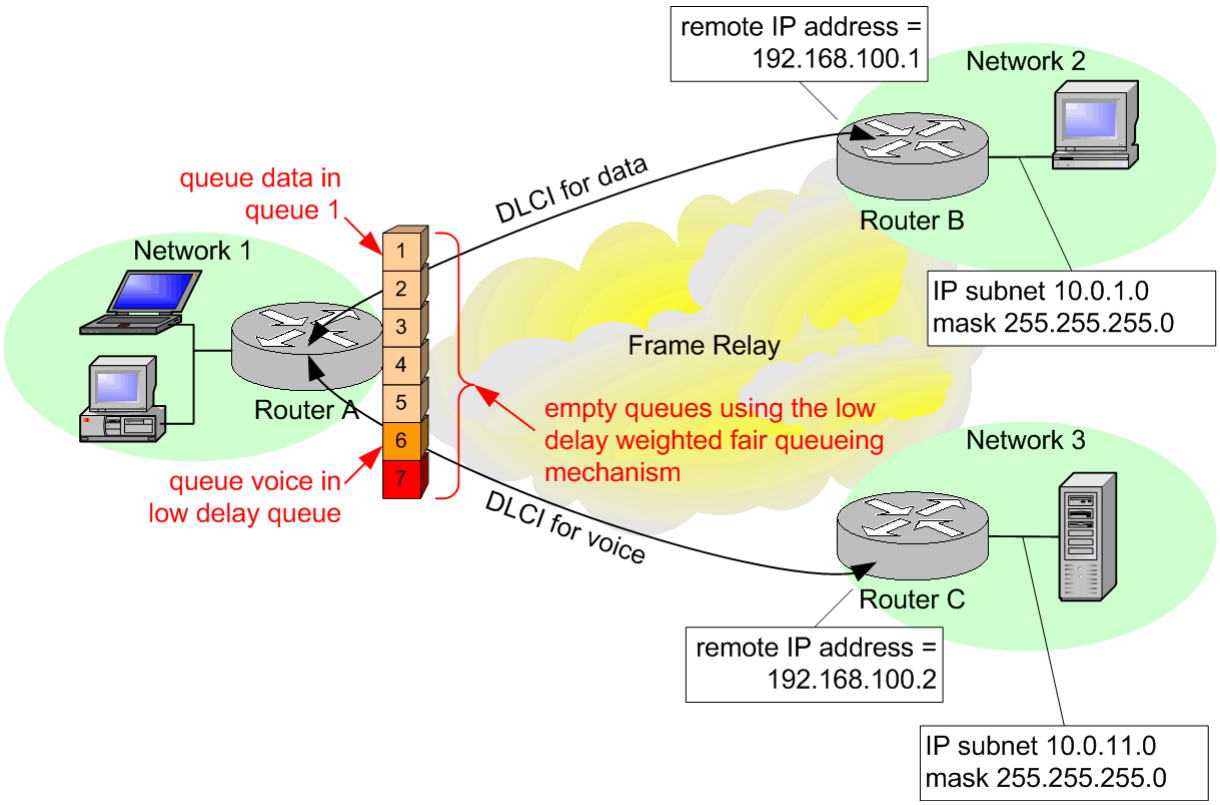
Etape	Action
1	Créer un … • DLCI à Frame Relay. Reportez-vous à MU-6.3.2 - Configuration de DLCI de Frame Relay page 111. ou • liaison PPP multiple. Reportez-vous à MU-6.4.13 - Configuration de PPP multiclasses page 141.
2	Dans la table dlciTable (Frame Relay) ou multiclassInterfaces (PPP), réglez l'élément defaultQueue sur la file d'attente souhaitée (p. ex. queue3). ⇒En cas de surcharge, cette file sera remplie par les données en excédent.
3	Il vous reste encore à créer et à appliquer une politique de priorité pour vider la file. Procédez comme cela est décrit dans MU-7.8.6 - Création d'une politique de priorité page 213 et MU-7.8.7 - Application d'une politique de priorité sur une interface page 215.

La figure qui suit montre où est situé l'attribut defaultQueue:



Exemple - configuration d'une file par défaut

Supposons que vous ayez un réseau connecté à deux autres réseaux par une ossature à Frame Relay. Le réseau 1 transporte un mélange de trafic de données et de trafic vocal. Vous voulez que le trafic de données soit acheminé du réseau 1 au réseau 2 et que le trafic vocal soit acheminé du réseau 1 au réseau 3. En cas de congestion, vous voulez que les données soient mises dans la file 1 et que la voix soit mise en file d'attente à faible temporisation. L'algorithme que vous souhaitez utiliser pour vider les files est le mécanisme de mise en file d'attente à faible temporisation pondéré.

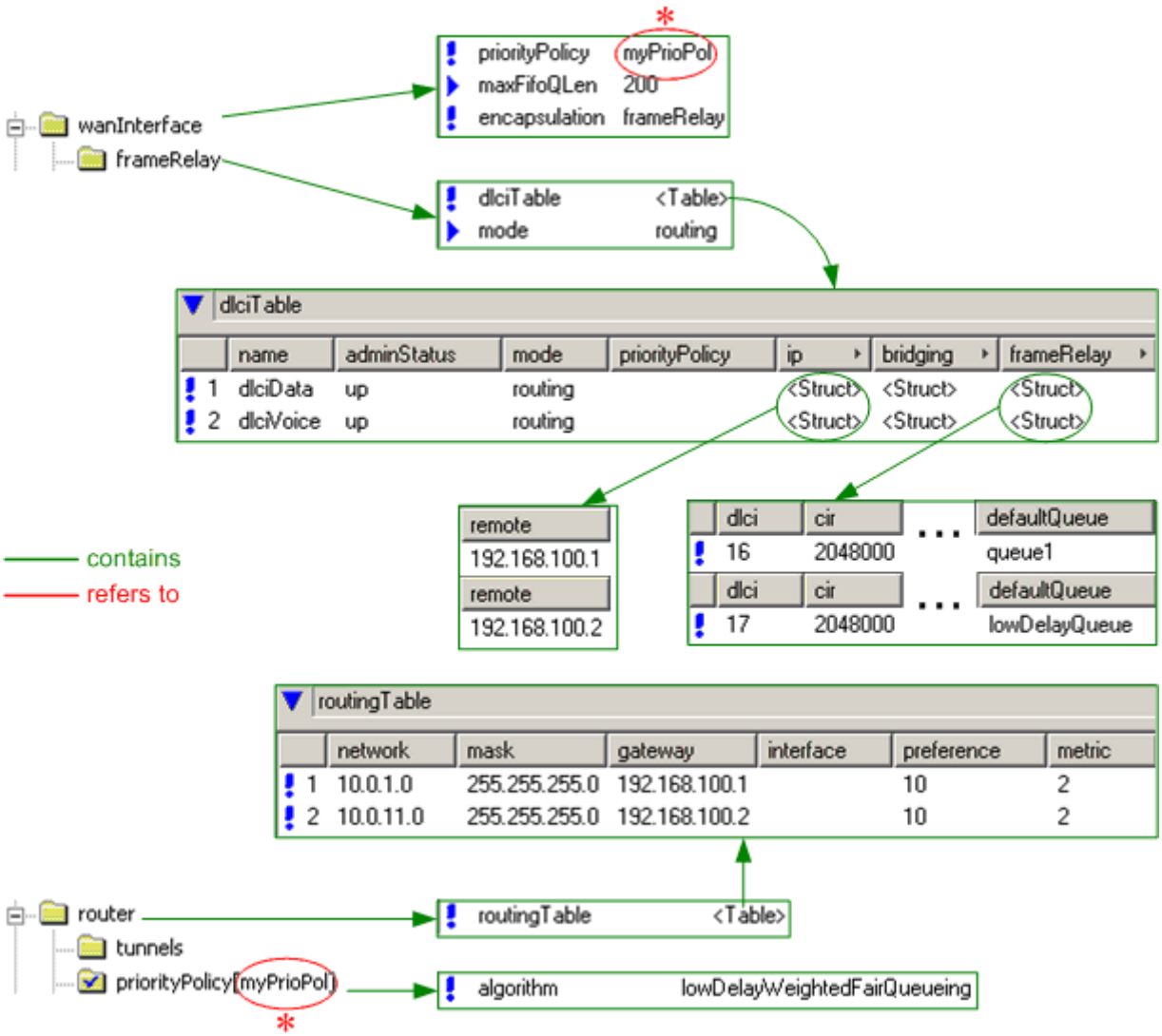


A grands traits, voici comment configurer cette disposition:

Etape	Action
1	Configurez deux DLCI à Frame Relay. Par exemple: • Configurez un DLCI à Frame Relay qui transportera le trafic de données, p. ex. dlciTable/name = dataDlci. • Configurez un autre DLCI à Frame Relay qui transportera le trafic vocal, p. ex. dlciTable/name = voiceDlci. Puisque ce n'est pas le sujet principal de cet exemple, reportez-vous, pour de plus amples informations sur la création de DLCI à Frame Relay, à MU-6.3.2 - Configuration de DLCI de Frame Relay page 111.
2	Définissez la file par défaut correcte pour les DLCI que vous avez créés, c'est-à-dire la file 1 pour le DLCI de données et la file 6 (la file à faible temporisation) pour le DLCI vocal.
3	Créez et appliquez une politique de priorité. La politique de priorité utilise le mécanisme de mise en file d'attente à faible temporisation pondéré pour vider les files.

Etape	Action
4	Créez des trajets vers les autres réseaux.

La figure qui suit montre comment configurer la politique de trafic et de priorité que vous souhaitez:



MU-8 Configuration du pontage

Ce chapitre présente le pontage sur le Routeur Telindus 1421 SHDSL et répertorie les attributs que vous pouvez utiliser pour configurer le pontage.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-8.1 - Introduction au pontage page 225
- MU-8.2 - Configuration du pontage page 236
- MU-8.3 - Configuration de la politique de trafic et de priorité sur le pont page 247

Reportez-vous au Manuel de référence pour un aperçu complet des attributs du Routeur Telindus 1421 SHDSL.

MU-8.1 Introduction au pontage

Cette section introduit le concept de pontage. Le tableau suivant donne un aperçu de ce chapitre:

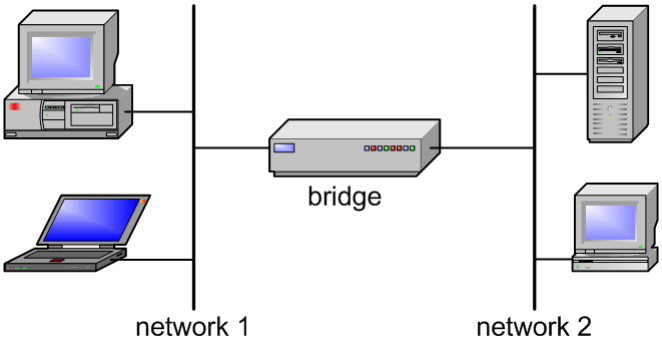
- MU-8.1.1 - Qu'est-ce que le pontage? page 226
- MU-8.1.2 - Le pont à auto-apprentissage et le Transparent Spanning Tree page 227
- MU-8.1.3 - Le pont racine Spanning Tree page 228
- MU-8.1.4 - Topologie du Spanning Tree page 229
- MU-8.1.5 - Etats des ports de pontage du Spanning Tree page 230
- MU-8.1.6 - La BPDU du Spanning Tree page 232
- MU-8.1.7 - Comportement du Spanning Tree page 233
- MU-8.1.8 - Priorité et coût du Spanning Tree page 234

MU-8.1.1 Qu'est-ce que le pontage?

Le Routeur Telindus 1421 SHDSL peut être configuré pour fonctionner comme un pont. Cela vous permet de diviser votre réseau LAN en parties plus petites, ou segments. Cela réduit l'importance du trafic de données sur les différents segments du LAN et, en conséquence, augmente la largeur de bande disponible.

Exemple:

La figure qui suit donne un exemple de pontage:



Les données provenant du réseau 1 ne peuvent franchir le pont que si elles ont une destination en dehors du réseau 1 ou si elles ont une adresse de diffusion ou de multidiffusion. Cela signifie que le pont filtre les données et réduit le trafic de données sur les divers segments du LAN.

MU-8.1.2 Le pont à auto-apprentissage et le Transparent Spanning Tree

Le Routeur Telindus 1421 SHDSL propose deux mécanismes de pontage:

- pontage à auto-apprentissage.
- pontage à auto-apprentissage couplé à l'algorithme Transparent Spanning Tree (TST), ou, en bref, pontage Spanning Tree.

Principe de pontage	Description
auto-apprentissage	Le pont apprend quelles données il doit transmettre à l'autre segment LAN et quelles données il doit bloquer. Il construit sa propre table de pontage. En d'autres termes, vous ne devez pas configurer une table de pontage avec les adresses des stations MAC situées sur les segments LAN distincts, mais qui doivent communiquer ensemble.
auto-apprentissage + TST	Cette méthode est basée sur le principe de l'auto-apprentissage, mais un protocole est utilisé pour mettre en œuvre l'algorithme TST. **Boucles de pontage** L'objectif premier de cet algorithme est d'éviter que des boucles de pontage se produisent. Une boucle de pontage se produit lorsque deux ponts à auto-apprentissage sont disposés en parallèle. Cela empêche les données de circuler en boucle, chaque pont transmettant les mêmes données. **L'algorithme TST** Grâce à l'algorithme TST, les ponts connaissent leur existence mutuelle. En communiquant les uns avec les autres, ils établissent un trajet unique pour atteindre un segment de réseau spécifique. Si nécessaire, ils peuvent décider de désactiver certains ponts du réseau afin de déterminer ce trajet unique. C'est un processus continu. Ainsi, si un pont est défaillant, les ponts restants reconfigurent leurs tables de pontage en laissant chaque segment LAN joignable.

MU-8.1.3 Le pont racine Spanning Tree

Qu'est-ce que le pont racine?

Le Spanning Tree définit un arbre avec un pont racine et un trajet sans boucle allant de la racine à l'ensemble des ponts du réseau étendu. Le pont racine est le centre logique de la topologie du Spanning Tree.

Les trajets de données redondants sont placés en mode de veille (bloqué). Si un segment de réseau dans le Spanning Tree est défaillant et qu'un trajet redondant existe, l'algorithme du Spanning Tree recalcule la topologie et active le trajet en veille.

Comment sélectionner un pont racine?

Tous les ponts du réseau participant au Spanning Tree collectent des informations sur les autres ponts du réseau. Ils le font en échangeant des messages de données appelés Bridge Protocol Data Units (BPDU).

Cet échange de messages entraîne les phases suivantes:

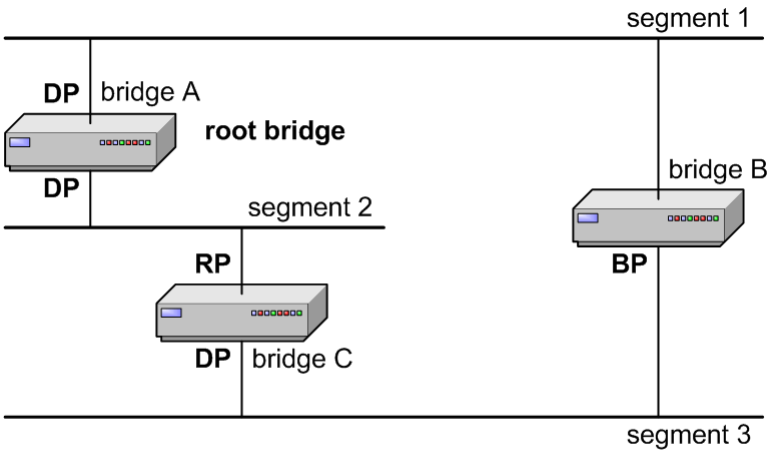
Phase	Description
1	Sélection d'un pont racine Le pont ayant la plus haute priorité de pont (c'est-à-dire la plus petite valeur de priorité numérique) est sélectionné comme pont racine. Si tous les ponts sont configurés avec la priorité par défaut (32768), le pont ayant l'adresse MAC la moins élevée devient le pont racine.
2	Sélection d'un pont spécifique pour chaque segment LAN ponté.
3	Suppression des boucles dans le réseau ponté en bloquant les ports de pont connectés aux liaisons redondantes.

MU-8.1.4 Topologie du Spanning Tree

Le facteur coût est utilisé pour calculer la distance entre chaque port d'un pont et le pont racine. Sur cette base, chaque port d'un pont se voit affecter l'un des états suivants:

Etat	Description
port racine	Le port le plus proche du pont racine. Un seul port de chaque pont est affecté comme port racine.
port désigné	Le port connecté à des ponts plus éloignés du pont racine. Le pont racine a uniquement des ports désignés.
blocage	Si un port n'a aucun port racine affecté ni aucun état de port désigné, un état de blocage lui est affecté. Les trames (à l'exception des BPDU de configuration) ne sont ni acceptées ni transmises par le port lorsqu'il est en état de blocage. On dit alors que le port est en état de veille.

La figure ci-dessous fournit un exemple élémentaire de topologie de Spanning Tree:



RP = Root Port
DP = Designated Port
BP = Blocking Port

MU-8.1.5 Etats des ports de pontage du Spanning Tree

Etats des ports de pontage

Un port de pontage peut avoir quatre états:

Etat	Un port ayant cet état…
blocage	• ne transmet aucune trame. • n'intègre pas la localisation de station dans sa base de données d'adressage (aucun apprentissage sur un port de blocage, donc aucune mise à jour de la base de données d'adresse MAC). • reçoit des BPDU, mais ne les traite pas et ne les transmet pas. Un pont est toujours en état de blocage à la suite d'une initialisation de pont.
écoute	• ne transmet aucune trame. • n'intègre pas la localisation de station dans sa base de données d'adressage (aucun apprentissage sur un port d'écoute, donc aucune mise à jour de la base de données d'adresse MAC). • reçoit et traite les BPDU, mais ne les transmet pas.
apprentissage	• ne transmet aucune trame. • intègre la localisation de station dans la base de données d'adressage MAC. • reçoit, traite et transmet les BPDU.
transmission	• transmet les trames. • intègre la localisation de station dans la base de données d'adressage MAC. • reçoit, traite et transmet les BPDU.

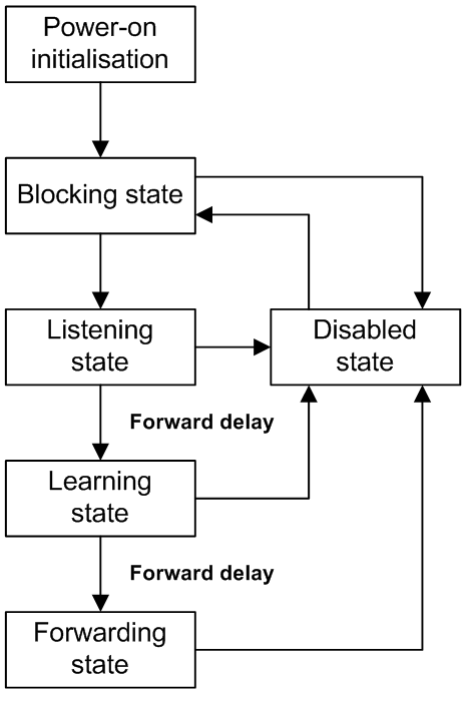
Diagramme de transition d'état de port de pontage

La figure qui suit montre comment un port de pontage passe par les différents états lorsque le pont est activé:

Lorsque vous activez le Spanning Tree, chaque pont du réseau passe par les états transitoires de l'écoute et de l'apprentissage lors de la mise sous tension. S'il est correctement configuré, chaque port se stabilise en état de transmission ou de blocage.

Lorsque l'algorithme de Spanning Tree place un port en état de transmission, le processus suivant se déclenche:

1. Le port est mis en état d'écoute pendant qu'il attend les informations de protocole qui lui suggèrent de passer en état de blocage.
2. Le port attend l'expiration du délai de transmission, passe en état d'apprentissage et réinitialise le délai de transmission.
3. En mode apprentissage, le port continue de bloquer la transmission des trames tant qu'il acquiert les informations de localisation de station pour la base de données de transmission.



4. Le port attend l'expiration du délai de transmission et passe en état de transmission. L'apprentissage et la transmission sont alors activés.

MU-8.1.6 La BPDU du Spanning Tree

Qu'est-ce qu'une BPDU?

Pour définir un trajet stable, chaque pont envoie des BPDU (Configuration Bridge Protocol Data Units) aux ponts voisins. Ces messages de BPDU de configuration contiennent des informations sur la topologie du Spanning Tree. Le contenu de ces trames varie uniquement lorsque la topologie du réseau ponté change ou n'a pas été définie.

Chaque BPDU de configuration contient au minimum les informations suivantes:

- l'identificateur unique du pont que le pont de transmission pense être un pont racine.
- le coût du trajet du port racine au port de transmission.
- l'identificateur unique du port de transmission.

Lorsqu'un pont transmet une trame BPDU, tous les ponts connectés au LAN sur lequel la trame est transmise reçoivent la BPDU. Lorsqu'un pont reçoit une BPDU, il ne transmet pas la trame. Au lieu de cela, il utilise les informations de la trame pour:

- calculer une BPDU,
- initier une transmission de BPDU si la topologie change.

Propagation des BPDU de configuration

Si un réseau ponté est en état stable, les commutations se poursuivent pour envoyer les BPDU de configuration aux ponts voisins à intervalles réguliers. Les BPDU de configuration sont transmises par le Spanning Tree des ports désignés aux ports racines. Si une BPDU de configuration n'est pas reçue par le port racine d'un pont dans un délai prédéfini (par exemple parce qu'un pont le long du trajet est défaillant), le port passe en état d'écoute pour redéfinir un trajet stable.

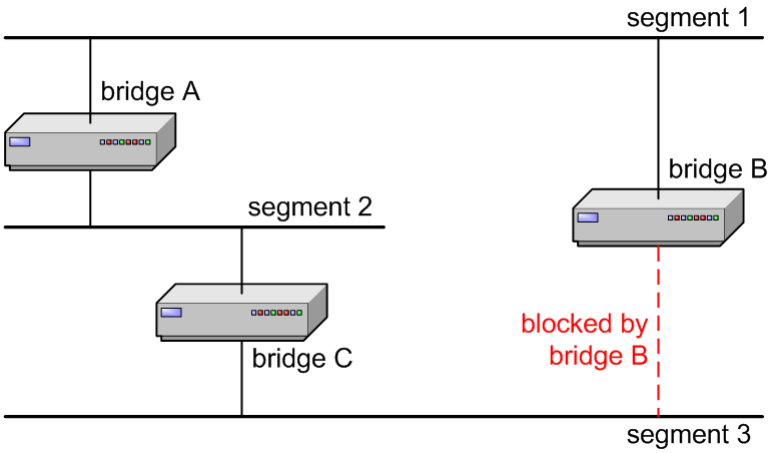
MU-8.1.7 Comportement du Spanning Tree

Les paragraphes qui suivent donnent quelques exemples du comportement du Spanning Tree lorsque certains événements surviennent dans votre réseau.

Boucles de pontage

Les ponts connectés à un LAN doivent détecter des boucles de pont potentielles. Ils doivent ensuite supprimer ces boucles en bloquant les ports appropriés vers d'autres ponts.

Cela est illustré par la figure qui suit:

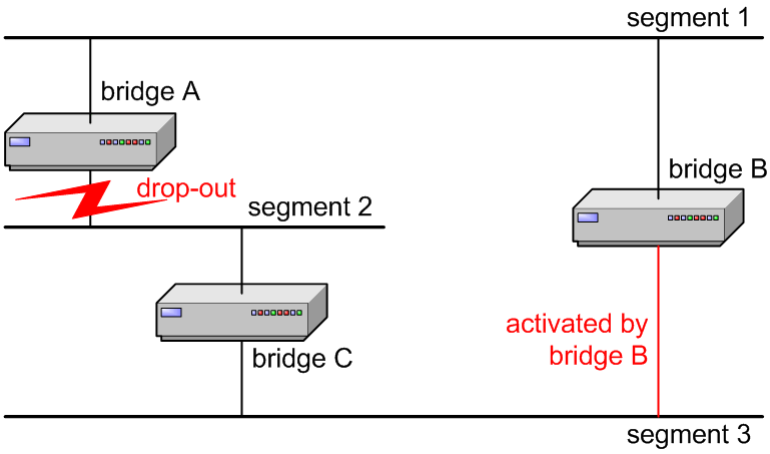


un trajet alternatif a été défini en connectant le pont B en parallèle avec les ponts A et C. Cela crée également une boucle de pont potentielle. Toutefois, en utilisant l'algorithme du Spanning Tree, le pont B rompt la boucle et bloque son trajet vers le segment 3.

Défaillance de pont

Les ponts connectés à un LAN doivent détecter des défaillances de boucles. Ils doivent alors définir un trajet de rechange. Si le pont racine s'avère défaillant, un nouveau pont racine doit être sélectionné.

Une défaillance de pont est illustrée par la figure qui suit:

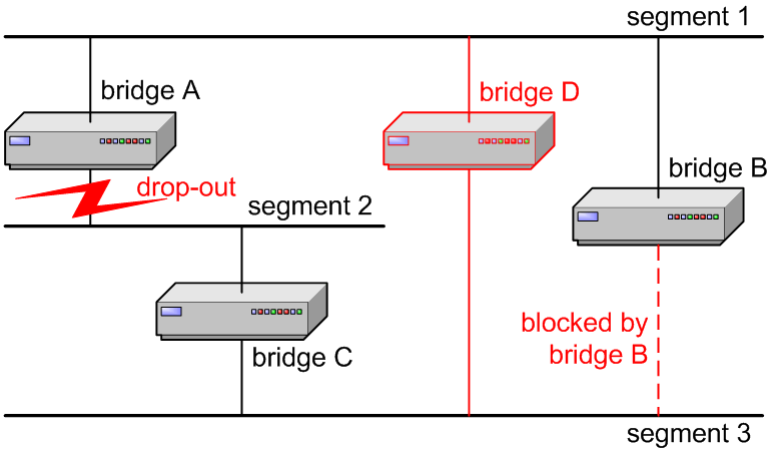


Si le pont A tombe en panne, l'algorithme du Spanning Tree doit être capable d'activer un trajet alternatif, tel que le pont B.

Extension de réseau

Les ponts connectés à un LAN doivent détecter des changements de topologie. Ils doivent s'adapter à ces changements.

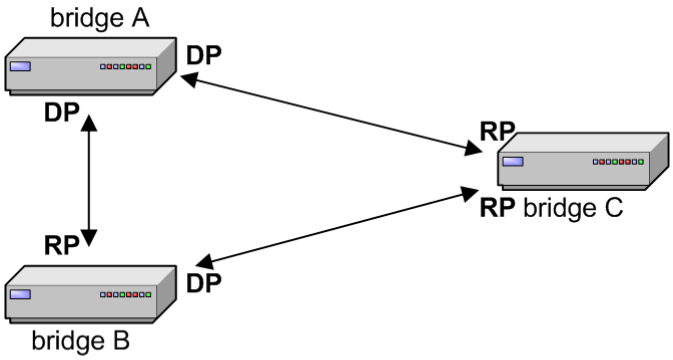
Un changement de topologie est illustré par la figure qui suit:



Si le réseau est étendu par l'ajout du pont D, l'algorithme du Spanning Tree doit être capable de s'adapter automatiquement à cette nouvelle topologie. Cela signifie que le pont B interrompt la boucle en bloquant le trajet vers le segment 3.

MU-8.1.8 Priorité et coût du Spanning Tree

Prenons la topologie de Spanning Tree suivante:



RP = Root Port
DP = Designated Port

Qu'est-ce que la priorité de pont?

Dans l'exemple ci-dessus, le pont A est choisi comme pont racine. Cela parce que la priorité de tous les ponts est la valeur par défaut (32768) et que le pont A a l'adresse MAC la plus basse. Toutefois, du fait des modèles de trafic ou des types de liaison, le pont A peut ne pas être le pont racine idéal.

En augmentant la priorité de pont (en abaissant la valeur de priorité numérique) du pont idéal de telle manière qu'il devienne le pont racine, vous provoquez un nouveau calcul du Spanning Tree, donnant une nouvelle topologie dans laquelle le pont idéal est la racine.

Que sont la priorité de port et le coût du trajet?

Lorsque la topologie du Spanning Tree est calculée sur la base des paramètres par défaut, le trajet entre la station source et la station de destination au sein d'un réseau ponté peut ne pas être idéal. Le but est de constituer la liaison la plus rapide avec le port racine.

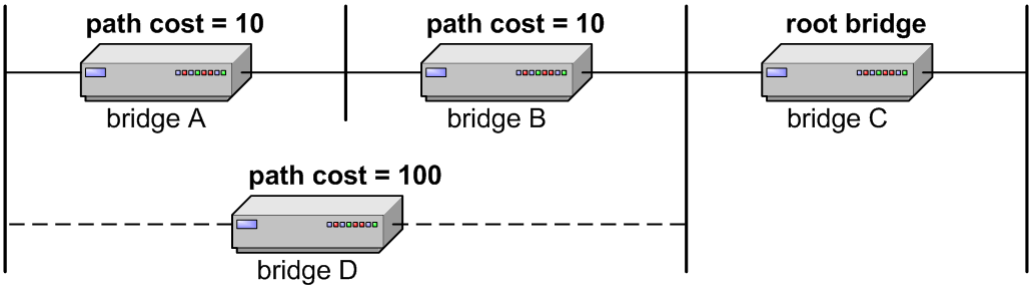
Par exemple, prenons un pont B sur lequel…

- le port 1, qui est le port racine actuel, est une liaison par paire torsadée non blindée,
- le port 2 est une liaison par fibres optiques.

Le trafic sur le réseau pourrait être plus efficace par la liaison en fibres optiques à grande vitesse. En modifiant la priorité du port ou le coût du trajet dans le Spanning Tree pour le port 2 vers une priorité plus élevée (moindre valeur numérique) que celle du port 1, le port 2 devient le port racine.

Exemple:

En modifiant l'attribut priority et/ou pathCost, vous pouvez créer un "trajet préférentiel":



en réglant les coûts de trajet des ponts A et B sur une valeur inférieure à celle du pont D, vous pouvez créer un trajet *préférentiel* par les ponts A et B. Le trajet par le pont D devient alors le trajet *de secours*.

MU-8.2 Configuration du pontage

Cette section répertorie les attributs que vous pouvez utiliser pour configurer le pontage. Le tableau suivant donne un aperçu de ce chapitre:

- MU-8.2.1 - Présentation des attributs de pontage page 237
- MU-8.2.2 - Configuration du groupe de pontage page 238
- MU-8.2.3 - Ajout d'un groupe de pontage page 239
- MU-8.2.4 - Activation du pontage sur une interface page 241
- MU-8.2.5 - Configuration du pontage sur une interface page 242
- MU-8.2.6 - Explication de la structure bridging page 243

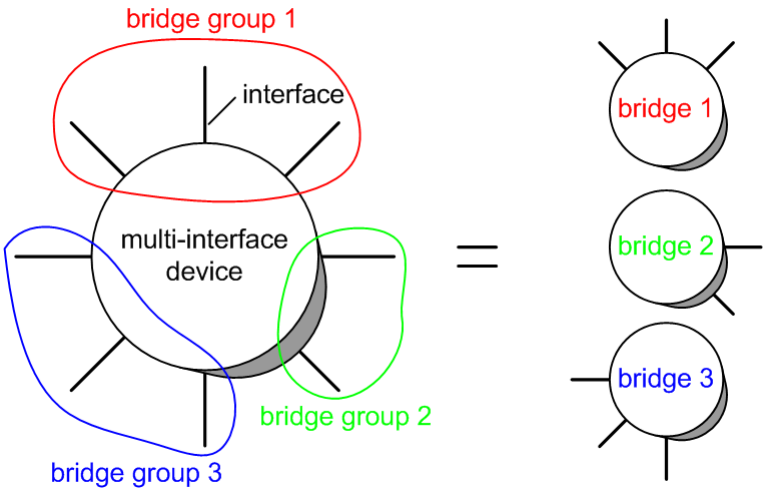
MU-8.2.1 Présentation des attributs de pontage

Qu'est-ce qu'un groupe de pontage?

Un groupe de pontage se compose des principaux processus de pontage. Ainsi, dans l'arborescence, l'objet bridgeGroup contient les attributs généraux de pontage.

Que sont les groupes de pontage multiples?

Le Routeur Telindus 1421 SHDSL offre la possibilité de créer des groupes de pontage multiples. Cela signifie que vous pouvez grouper certaines interfaces dans un groupe de pontage tout en groupant certaines autres interfaces dans un autre groupe. Ce faisant, c'est comme si vous créiez plusieurs unités de pontage “simples” au sein d'une seule unité.



Pontage sur les différentes interfaces

En plus de pouvoir configurer le processus général de pontage en utilisant les attributs de configuration du groupe de pontage, vous devez également configurer le pontage sur chaque interface sur laquelle vous souhaitez utiliser le pontage.

MU-8.2.2 Configuration du groupe de pontage

Reportez-vous au…

- MU-8.1 - Introduction au pontage page 225 pour une introduction au pontage.
- MU-8.2.1 - Présentation des attributs de pontage page 237 pour une introduction aux attributs de pontage.

Cette section répertorie les attributs de configuration les plus importants du groupe de pontage.

Configuration d'une adresse IP sur le groupe de pontage

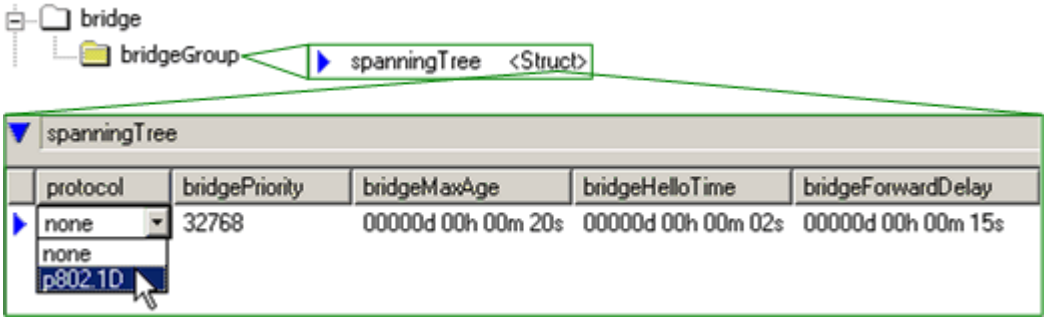
Comme sur une autre interface (LAN, PVCs, etc.), vous pouvez configurer une adresse IP sur le groupe de pontage. Faites-le en utilisant l'attribut de configuration telindus1421Router/bridge/bridgeGroup/ip page 145.

De plus, si vous activez le pontage sur l'interface LAN (telindus1421Router/lanInterface/mode = bridging), les réglages de l'attribut de configuration telindus1421Router/lanInterface/ip sont ignorés. Dans ce cas, si vous souhaitez gérer le Routeur Telindus 1421 SHDSL via IP, vous devez configurer une adresse IP dans l'objet bridgeGroup.

Sélection du protocole de pontage

Reportez-vous à MU-8.1.2 - Le pont à auto-apprentissage et le Transparent Spanning Tree page 227 pour la présentation.

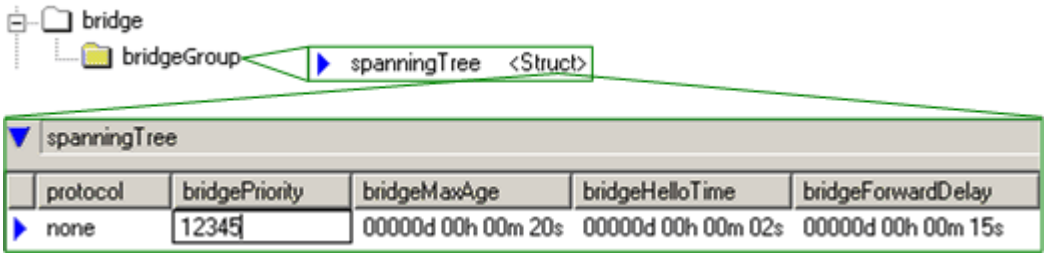
Utilisez l'élément protocol dans la structure du spanningTree pour sélectionner le protocole de pontage. Reportez-vous à telindus1421Router/bridge/bridgeGroup/spanningTree page 147.



Réglage de la priorité de pontage

Reportez-vous à MU-8.1.8 - Priorité et coût du Spanning Tree page 234 pour de plus amples informations sur la priorité de pontage.

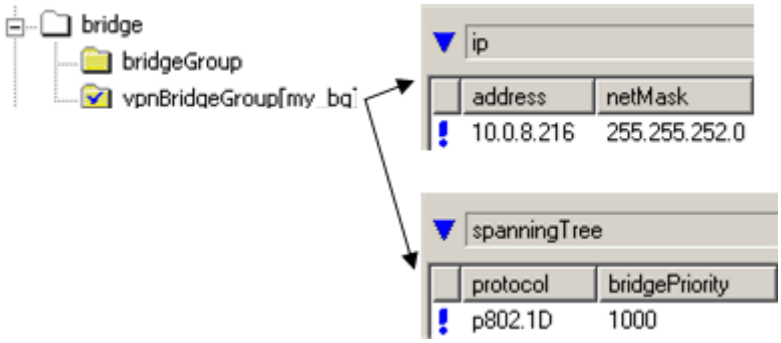
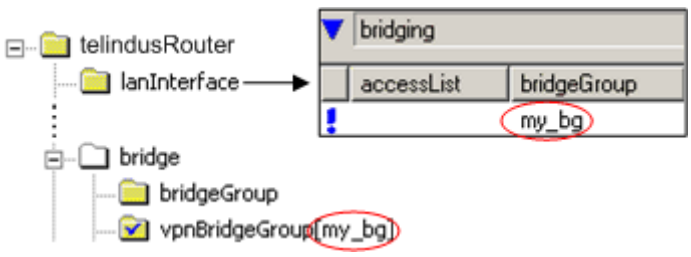
Utilisez l'élément bridgePriority dans la structure du spanningTree pour sélectionner la priorité de pontage. Reportez-vous à telindus1421Router/bridge/bridgeGroup/spanningTree page 147.



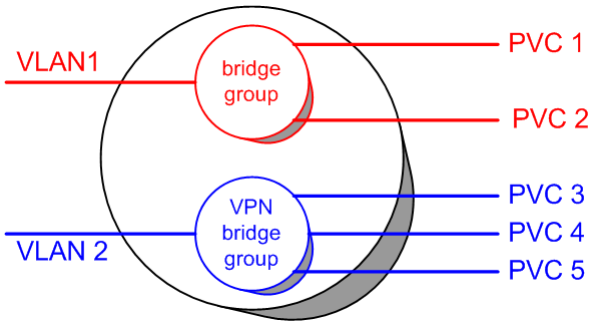
MU-8.2.3 Ajout d'un groupe de pontage

Comme nous l'avons vu dans MU-8.2.1 - Présentation des attributs de pontage page 237, vous pouvez ajouter plusieurs groupes de pontage.

Pour ajouter un groupe de pontage, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet bridge et ajoutez un objet vpnBridgeGroup[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43). P. ex. vpnBridgeGroup[my_bg]
2	Dans l'objet vpnBridgeGroup[ ] que vous venez d'ajouter, configurez les attributs en fonction de vos besoins. Exemple: Supposons que vous configuriez une adresse IP sur le groupe de pontage, activez le protocole du Spanning Tree et définissez une priorité de pontage. 
3	Vous pouvez maintenant ajouter des interfaces au groupe de pontage que vous venez de créer. Pour ce faire, entrez le nom du groupe de pontage dans l'élément bridging/ bridgeGroup de l'interface que vous souhaitez ajouter. Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 (plus spécifiquement à l'élément bridgeGroup) pour de plus amples informations. Exemple: Supposons que vous souhaitiez ajouter l'interface LAN à l'objet vpnBridgeGroup[my_bg] que vous avez ajouté précédemment. Entrez alors la chaîne “my_bg” dans l'élément bridgeGroup de la structure bridging de l'objet lanInterface. 

Exemple – groupes de pontage multiples

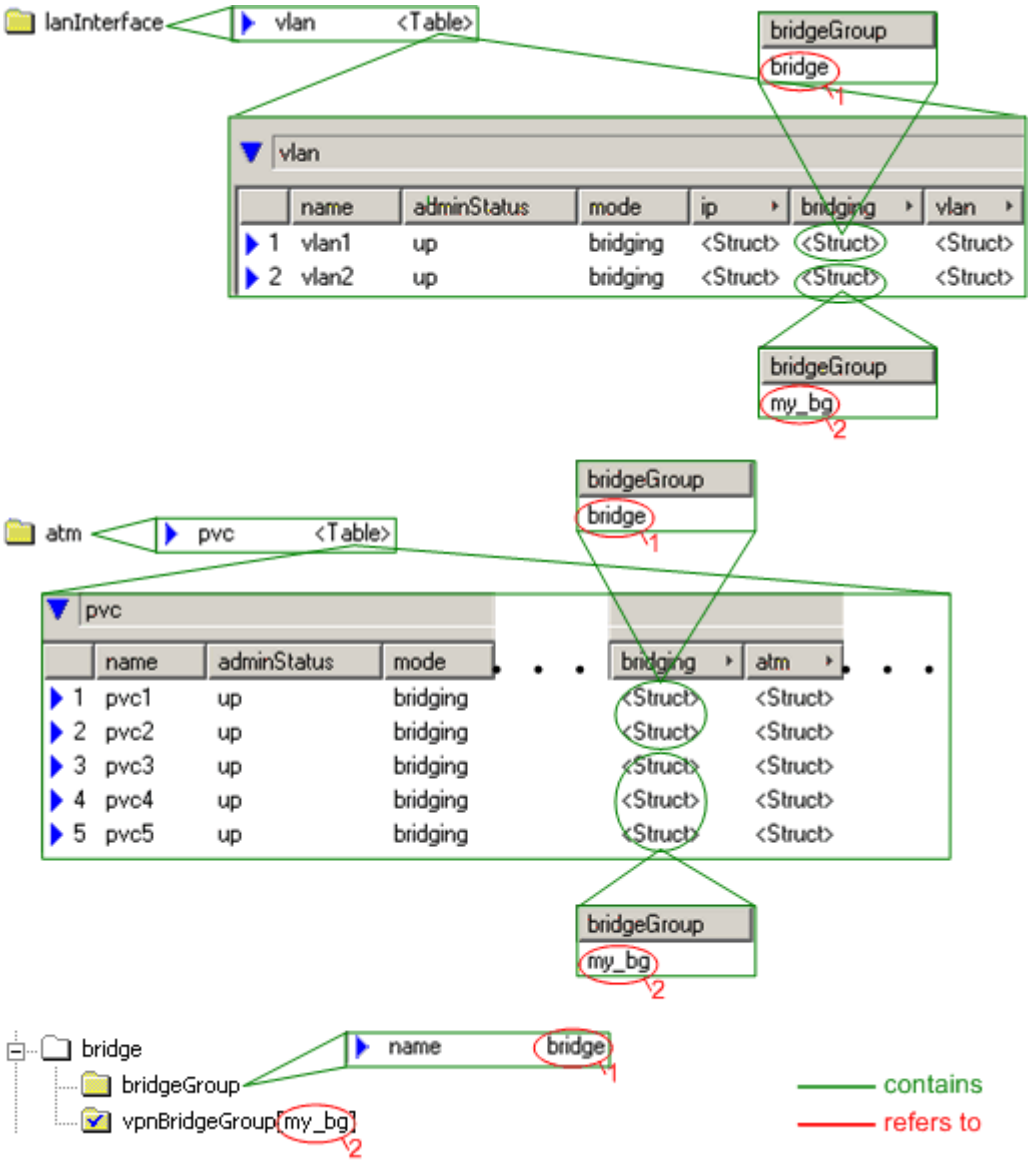


Supposons…

- que vous disposez de 2 VLAN (VLAN 1 et VLAN 2).
- que vous disposiez de 5 PVC (PVC 1 à PVC 5).
- que vous souhaitiez affecter VLAN 1 et PVC 1 et 2 au groupe de pontage par défaut.
- que vous souhaitiez affecter VLAN 2 et PVC 3, 4 et 5 à un groupe de pontage que vous avez ajouté vous-même.

Premièrement, ajoutez un groupe de pontage dans l'arborescence (p. ex. vpnBridgeGroup[my_bg]. Affectez ensuite les différentes interfaces aux différents groupes de pontage en spécifiant les noms de ces groupes dans les éléments bridging/bridgeGroup des différentes interfaces. Déterminez les différentes interfaces en mode de pontage.

La configuration est la suivante:



MU-8.2.4 Activation du pontage sur une interface

Reportez-vous au…

- MU-8.1 - Introduction au pontage page 225 pour une introduction au pontage.
- MU-8.2.1 - Présentation des attributs de pontage page 237 pour une introduction aux attributs de pontage.

Pour chaque interface IP, vous pouvez déterminer si vous procédez à un acheminement, un pontage, ou les deux. Le tableau suivant montre, pour chaque interface IP, comment activer le pontage:

Interface	Comment activer le pontage?
Interface LAN	Réglez l'attribut mode sur bridging ou routingAndBridging. L'attribut mode se trouve dans l'objet lanInterface: telindus1421Router/lanInterface/mode. **Remarque importante** Si vous réglez l'attribut de configuration telindus1421Router/lanInterface/mode sur bridging, alors le réglage de l'attribut de configuration telindus1421Router/lanInterface/ip est ignoré. Dans ce cas, si vous souhaitez gérer le Routeur Telindus 1421 SHDSL via IP, vous devez configurer une adresse IP dans l'objet bridgeGroup. telindus1421Router/bridge/bridgeGroup/ip.
VLAN sur l'interface LAN	Réglez l'élément mode sur bridging ou routingAndBridging. L'élément mode se trouve dans la table vlan qui est située dans l'objet lanInterface: telindus1421Router/lanInterface/vlan/mode.
ATM PVC	Réglez l'élément mode sur bridging ou routingAndBridging. L'élément mode se trouve dans la table pvcTable qui est située dans l'objet atm: telindus1421Router/wanInterface/atm/pvcTable/mode.
Liaison PPP	Réglez l'élément mode sur bridging ou routingAndBridging. L'élément mode se trouve dans l'objet ppp: telindus1421Router/wanInterface/ppp/mode.
PVC relais trame	Réglez l'élément mode sur bridging ou routingAndBridging. L'élément mode se trouve dans la table dlciTable qui est située dans l'objet frameRelay: telindus1421Router/wanInterface/frameRelay/dlciTable/mode.
Tunnel L2TP	Réglez l'élément mode sur bridging ou routingAndBridging. L'élément mode se trouve dans la table l2tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/l2tpTunnels/mode.
Tunnel IPSEC L2TP	Réglez l'élément mode sur bridging ou routingAndBridging. L'élément mode se trouve dans la table ipsecL2tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/ipsecL2tpTunnels/mode.

MU-8.2.5 Configuration du pontage sur une interface

Reportez-vous au…

- MU-8.1 - Introduction au pontage page 225 pour une introduction au pontage.
- MU-8.2.1 - Présentation des attributs de pontage page 237 pour une introduction aux attributs de pontage.

Une fois le processus de pontage activé sur l'interface (reportez-vous à MU-8.2.4 - Activation du pontage sur une interface page 241), vous pouvez configurer les paramètres de pontage de cette interface. Pour ce faire, utilisez les éléments de la structure bridging. La table qui suit vous indique l'emplacement de la structure bridging pour chaque interface:

Interface	Emplacement des paramètres IP
Interface LAN	Dans la structure bridging de l'objet lanInterface: telindus1421Router/lanInterface/bridging. **Remarque importante** Si vous réglez l'attribut de configuration telindus1421Router/lanInterface/mode sur bridging, alors le réglage de l'attribut de configuration telindus1421Router/lanInterface/ip est ignoré. Dans ce cas, si vous souhaitez gérer le Routeur Telindus 1421 SHDSL via IP, vous devez configurer une adresse IP dans l'objet bridgeGroup. telindus1421Router/bridge/bridgeGroup/ip.
VLAN sur l'interface LAN	Dans la structure bridging de la table vlan qui est située dans l'objet lanInterface: telindus1421Router/lanInterface/vlan/bridging.
ATM PVC	Dans la structure bridging de la table pvcTable qui est située dans l'objet atm: telindus1421Router/wanInterface/atm/pvcTable/bridging.
Liaison PPP	Dans la structure bridging de l'objet ppp: telindus1421Router/wanInterface/ppp/bridging.
PVC relais trame	Dans la structure bridging de la table dlciTable qui est située dans l'objet frameRelay: telindus1421Router/wanInterface/frameRelay/dlciTable/bridging.
Tunnel L2TP	Dans la structure bridging de la table 12tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/l2tpTunnels/bridging.
Tunnel IPSEC L2TP	Dans la structure bridging de la table ipsecL22tpTunnels qui est située dans l'objet tunnels: telindus1421Router/router/tunnels/ipsecL2tpTunnels/bridging.

Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 pour une explication détaillée de la structure bridging.

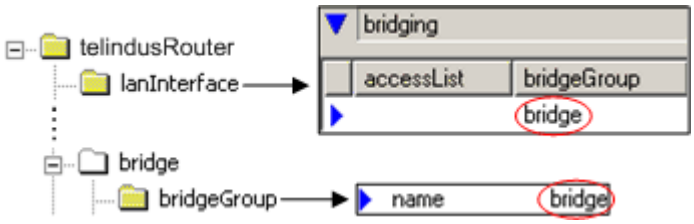
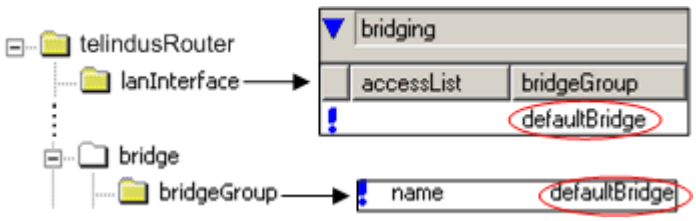
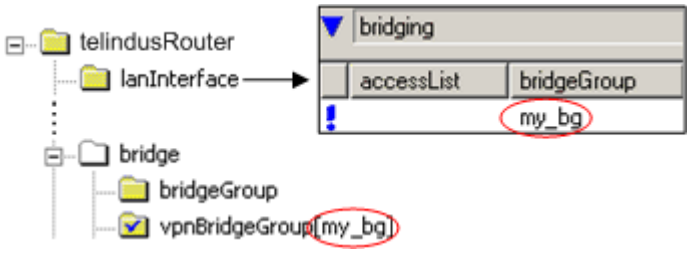
MU-8.2.6 Explication de la structure bridging

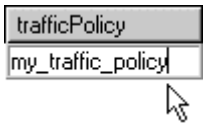
La structure bridging survenant dans plusieurs objets, elle ne sera décrite ici qu'une seule fois et mentionnée lorsque cela sera nécessaire. Reportez-vous à MU-8.2.5 - Configuration du pontage sur une interface page 242 pour l'emplacement de la structure de pontage.

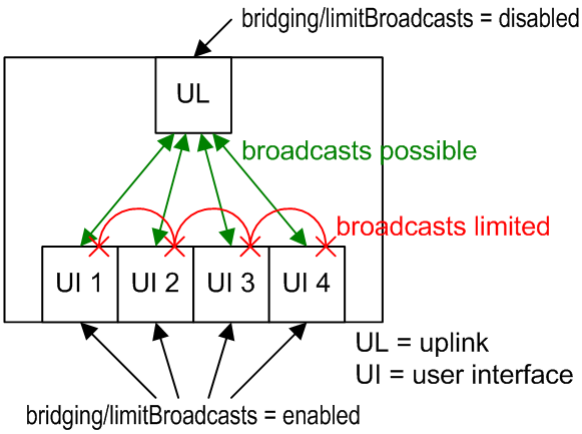
Cette section répertorie tous les éléments qui peuvent être présents dans la structure de pontage. Toutefois, en fonction de l'interface, il est possible que tous ces éléments ne soient pas présents.

La structure de pontage contient les éléments suivants:

Elément	Description
accessList	Utilisez cet élément pour configurer une liste d'accès sur l'interface. Par défaut:<néant> Gamme:0 … 24 caractères Pour ce faire, entrez le nom d'indice de la liste d'accès que vous souhaitez utiliser. Vous pouvez créer la liste d'accès elle-même en ajoutant un objet accessList sous l'objet bridge et en configurant les attributs dans cet objet. **Exemple:** Si vous avez créé un objet accessList avec le nom d'indice my_access_list (c'est-à-dire accessList[my_access_list]) et que vous souhaitez appliquer cette liste d'accès ici, entrez le nom d'indice comme valeur de l'élément accessList. Reportez-vous au… • MR-1.11.2 - Bridge access list configuration attributes page 152 pour de plus amples informations sur les listes d'accès. • MU-4.4 - Ajout d'un objet dans l'arborescence page 43 pour de plus amples informations sur l'ajout d'objets.

Elément	Description
bridgeGroup	Utilisez cet élément pour définir à quel groupe de pontage appartient l'interface. Par défaut:bridge Gamme:1 … 24 caractères Vous avez la possibilité de créer des groupes de pontage multiples (reportez-vous à MU-8.2.3 - Ajout d'un groupe de pontage page 239). Vous pouvez alors affecter certaines interfaces à un groupe de pontage tout en affectant plusieurs autres interfaces à un autre groupe de pontage. Par défaut, l'interface est affectée au groupe de pontage par défaut (à condition que l'attribut de configuration telindus1421Router/bridge/bridgeGroup/name du groupe de pontage par défaut possède toujours sa valeur par défaut "bridge"). Vous pouvez affecter l'interface à un groupe de pontage autre que le groupe par défaut en spécifiant le nom d'indice du groupe de pontage dans l'élément bridgeGroup. **Exemples** • Par défaut, l'élément bridgeGroup et l'attribut de configuration telindus1421Router/bridge/bridgeGroup/name du groupe de pontage par défaut sont définis sur "bridge". Cela signifie que par défaut, l'interface est affectée au groupe de pontage par défaut.  • Supposons que vous modifiez le nom du groupe de pontage par défaut (en modifiant la valeur de l'attribut de configuration telindus1421Router/bridge/bridgeGroup/name). Si vous souhaitez toujours affecter l'interface au groupe de pontage par défaut, vous devez entrer le nouveau nom du groupe par défaut dans l'élément bridgeGroup de l'interface.  • Supposons que vous ajoutiez un groupe de pontage portant le nom d'indice my_bg et que vous souhaitiez affecter l'interface à ce groupe de pontage, entrez le nom d'indice comme valeur de l'élément bridgeGroup. 

Elément	Description
trafficPolicy	Cet élément n'est pas présent dans la structure telindus1421Router/lanInterface/bridging. Utilisez cet élément pour appliquer une politique de trafic aux données pontées sur cette interface. Par défaut:<néant> Gamme:0 … 24 caractères Pour ce faire, entrez le nom d'indice de la politique de trafic que vous souhaitez utiliser. Vous pouvez créer la politique de trafic elle-même en ajoutant un objet trafficPolicy sous l'objet bridge et en configurant les attributs dans cet objet. **Exemple:** Si vous avez créé un objet trafficPolicy avec le nom d'indice my_traffic_policy (c'est-à-dire trafficPolicy[my_traffic_policy]) et que vous souhaitez appliquer cette politique de trafic ici, entrez le nom d'indice comme valeur de l'élément trafficPolicy.  Reportez-vous à MU-8.3 - Configuration de la politique de trafic et de priorité sur le pont page 247 pour de plus amples informations.
priorité	Utilisez cet élément pour définir la priorité de port de l'interface. Par défaut:128 Gamme:0 … 255 Chaque port d'un pont a un identificateur de port unique. L'élément priority est une partie de cet identificateur de port et vous permet de modifier la priorité du port. Il est considéré comme la partie la plus significative lors des comparaisons de priorité. L'autre partie de cet identificateur est fonction du port physique ou logique. Cela garantit le caractère unique de cet identificateur de port parmi tous les ports d'un pont. Reportez-vous à MU-8.1.8 - Priorité et coût du Spanning Tree page 234 pour de plus amples informations sur la priorité de port.
pathCost	Utilisez cet élément pour définir le coût de trajet de l'interface. Par défaut:100 Gamme:1 … 65535 Le coût du trajet est la valeur qui est ajoutée au coût total du trajet jusqu'au pont racine, à condition que ce port particulier soit un port racine, c'est-à-dire que le trajet jusqu'à la racine passe à travers ce port. Le coût total du trajet jusqu'au pont racine ne doit pas dépasser 65500. Reportez-vous à MU-8.1.8 - Priorité et coût du Spanning Tree page 234 pour de plus amples informations sur la priorité de port.
topologyChangeDetection	Utilisez cet élément pour activer ou désactiver la communication des changements de topologie du Spanning Tree jusqu'au pont racine. Par défaut:activé Gamme:activé / désactivé

Elément	Description
limitBroadcasts	Utilisez cet élément pour limiter les diffusions entre les interfaces pour lesquelles l'élément limitBroadcasts est réglé sur activé. Par défaut:désactivé Gamme:activé / désactivé **Exemple** Supposons que vous ayez la configuration suivante: • Quatre liaisons vers quatre utilisateurs différents (clients). • Une liaison montante vers l'ossature. • Toutes les liaisons sont configurées pour le pontage.  Dans ce cas, vous souhaitez probablement que les diffusions provenant de la liaison ascendante soient réparties vers les liaisons utilisateurs et que les diffusions provenant des liaisons utilisateurs soient transmises à la liaison ascendante. Toutefois, vous ne souhaitez vraisemblablement pas que les diffusions provenant d'une liaison utilisateur soient distribuées sur l'ensemble des autres liaisons utilisateurs. Par conséquent, réglez l'élément limitBroadcasts sur activé sur toutes les interfaces qui ne peuvent transmettre les diffusions.

MU-8.3 Configuration de la politique de trafic et de priorité sur le pont

Reportez-vous au…

- MU-7.8.1 - Présentation de la politique de trafic et de priorité page 205 pour une présentation de la politique de trafic et de priorité.
- MU-7.8.2 - Politique de trafic et de priorité sur les données acheminées et pontées page 208 pour la différence entre politique de trafic et politique de priorité sur le pont et sur le routeur.

Cette section donne une rapide description des attributs que vous pouvez utiliser pour configurer la politique de trafic et de priorité sur le pont.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-8.3.1 - Comment configurer une politique de trafic et de priorité sur le pont? page 248
- MU-8.3.2 - Configuration d'une politique de trafic sur le pont page 249
- MU-8.3.3 - Application d'une politique de trafic sur une interface donnée du pont page 250

MU-8.3.1 Comment configurer une politique de trafic et de priorité sur le pont?

Reportez-vous à MU-7.8.1 - Présentation de la politique de trafic et de priorité page 205 pour la présentation.

Pour configurer une politique de trafic et de priorité des données pontées sur une interface donnée, procédez de la façon suivante:

Etape	Action
1	Créez et configurez une politique de trafic de pontage. Reportez-vous à MU-8.3.2 - Configuration d'une politique de trafic sur le pont page 249.
2	Appliquez la politique de trafic de pontage à l'interface souhaitée. Reportez-vous à MU-8.3.3 - Application d'une politique de trafic sur une interface donnée du pont page 250.
3	Créez et configurez une politique de priorité. Reportez-vous à MU-7.8.6 - Création d'une politique de priorité page 213.
4	Appliquez la politique de priorité à l'interface souhaitée. Reportez-vous à MU-7.8.7 - Application d'une politique de priorité sur une interface page 215.

MU-8.3.2 Configuration d'une politique de trafic sur le pont

Reportez-vous à MU-8.3.1 - Comment configurer une politique de trafic et de priorité sur le pont? page 248 pour un aperçu de la manière de configurer une politique de trafic et de priorité. Pour vous permettre de suivre le processus, les points suivants vous en donnent un rapide aperçu.

- → **Créez et configurez une politique de trafic de pontage.** ← **Vous êtes ici.**
- Appliquez la politique de trafic de pontage à l'interface souhaitée.
- Créez et configurez une politique de priorité.
- Appliquez la politique de priorité à l'interface souhaitée.

Pour créer et configurer une politique de trafic des données pontées sur une interface donnée, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet bridge et ajoutez un objet trafficPolicy[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43). E.g. trafficPolicy[myBridgePol]
2	Dans l'objet trafficPolicy[ ] que vous venez d'ajouter, allez à l'attribut vlanPriorityMap. Utilisez cet attribut pour imposer une politique de trafic aux trames VLAN pontées reçues par le Routeur Telindus 1421 SHDSL. Reportez-vous à telindus1421Router/bridge/trafficPolicy[ ]/vlanPriorityMap page 155 pour de plus amples informations.
3	Dans l'objet trafficPolicy[ ] que vous venez d'ajouter, allez à l'attribut dropLevels. Utilisez cet attribut pour préciser, pour chaque file d'attente configurable par utilisateur, combien de paquets peuvent être mis en attente avant d'être envoyés. Reportez-vous à telindus1421Router/bridge/trafficPolicy[ ]/dropLevels page 155 pour de plus amples informations.

MU-8.3.3 Application d'une politique de trafic sur une interface donnée du pont

Reportez-vous à MU-8.3.1 - Comment configurer une politique de trafic et de priorité sur le pont? page 248 pour un aperçu de la manière de configurer une politique de trafic et de priorité. Pour vous permettre de suivre le processus, les points suivants vous en donnent un rapide aperçu.

- Créez et configurez une politique de trafic de pontage.
- → **Appliquez la politique de trafic de pontage sur l'interface souhaitée.** ← **Vous êtes ici.**
- Créez et configurez une politique de priorité.
- Appliquez la politique de priorité à l'interface souhaitée.

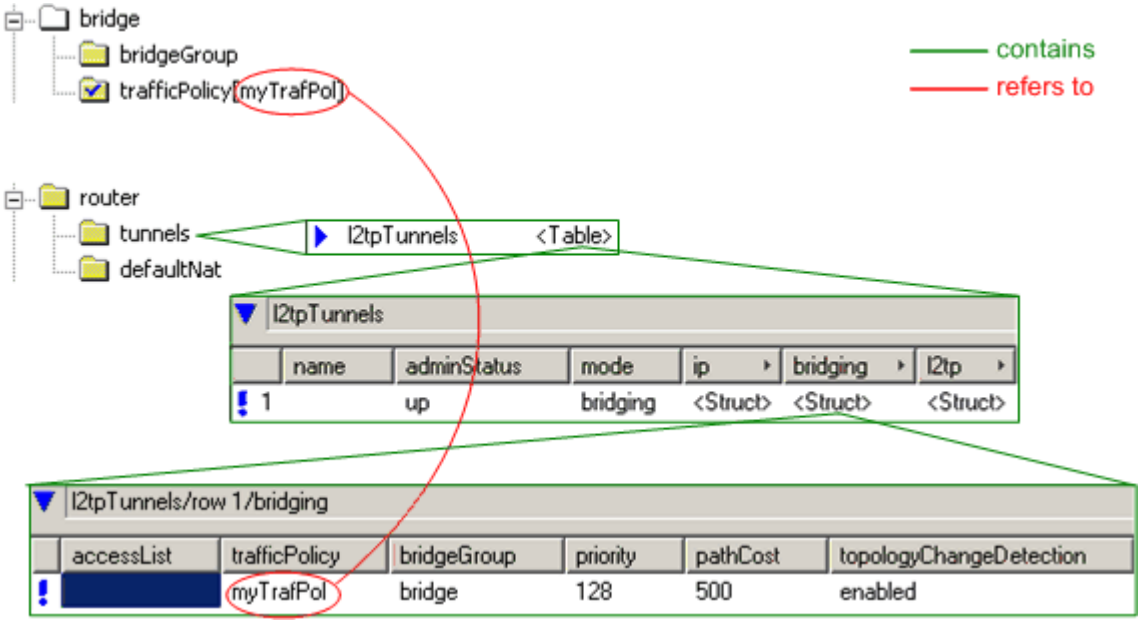
Pour appliquer une politique de trafic aux données pontées sur une interface donnée, entrez le nom d'indice de l'objet trafficPolicy[ ] créé auparavant comme valeur de l'élément trafficPolicy. L'élément trafficPolicy se trouve dans la structure bridging de l'interface IP. Reportez-vous à MU-8.2.5 - Configuration du pontage sur une interface page 242 pour l'emplacement de la structure de pontage sur les différentes interfaces IP.

Sur l'interface LAN, vous ne pouvez pas appliquer une politique de trafic de pontage.

Exemple – application d'une politique de trafic sur une interface du pont

Supposons que vous ayez créé et configuré un objet de politique de trafic avec le nom d'indice myTrafPol (c'est-à-dire trafficPolicy[myTrafPol]), et que vous souhaitiez appliquer cette politique de trafic à un tunnel L2TP créé auparavant.

La figure qui suit vous montre comment procéder à la configuration:



MU-9 Configuration des fonctions complémentaires

Ce chapitre présente les fonctions complémentaires les plus importantes du Routeur Telindus 1421 SHDSL outre l'acheminement, le pontage et la commutation, et répertorie les attributs utilisables pour configurer ces fonctions.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.1 - Configuration de DHCP page 253
- MU-9.2 - Configuration des restrictions d'accès page 258
- MU-9.3 - Configurer les VLAN page 271
- MU-9.4 - Configuration de tunnels L2TP page 278
- MU-9.5 - Configuration d'une sécurité IP page 285
- MU-9.6 - Configuration RADIUS page 291
- MU-9.7 - Configuration QoS page 297

Reportez-vous au Manuel de référence pour un aperçu complet des attributs du Routeur Telindus 1421 SHDSL.

MU-9.1 Configuration de DHCP

Cette section présente le Dynamic Host Configuration Protocol (DHCP) et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.1.1 - Introduction au DHCP page 254
- MU-9.1.2 - Assignation d'adresses IP statiques page 255
- MU-9.1.3 - Assignation d'adresses IP dynamiques page 256
- MU-9.1.4 - Configuration du Routeur Telindus 1421 SHDSL comme agent relais DHCP page 257

MU-9.1.1 Introduction au DHCP

Qu'est-ce que le DHCP?

Le protocole DHCP est un protocole qui permet d'assigner des adresses IP aux diverses unités d'un réseau. Le DHCP peut assigner des adresses IP dynamiques ou statiques. Avec l'adressage dynamique, une unité peut avoir une adresse IP différente chaque fois qu'elle se connecte au réseau. De plus, l'adresse IP peut varier pendant que l'unité est connectée.

L'adressage dynamique simplifie la gestion du réseau, parce que le logiciel conserve la trace des adresses IP sans qu'il soit besoin de demander à un administrateur réseau de gérer cette fonction. Cela implique qu'un nouvel ordinateur peut être ajouté à un réseau sans devoir lui affecter manuellement une adresse IP unique.

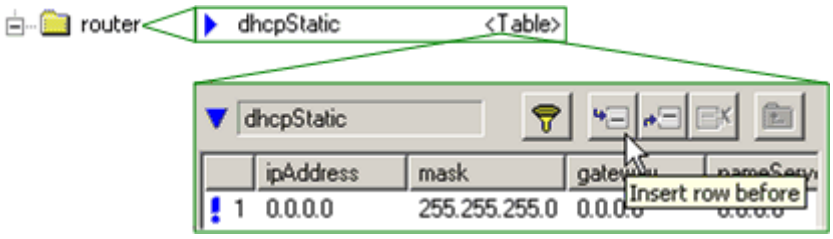
Qu'est-ce qu'un agent relais DHCP?

Etant un message diffusé, une demande DHCP ne peut franchir un routeur par défaut. Pour permettre à une demande DHCP de franchir le routeur, des adresses IP de secours doivent être configurées. Cela ajoute des informations supplémentaires au paquet de la demande, permettant aux serveurs de réseaux distants de renvoyer la réponse.

MU-9.1.2 Assignation d'adresses IP statiques

Reportez-vous à MU-9.1.1 - Introduction au DHCP page 254 pour la présentation.

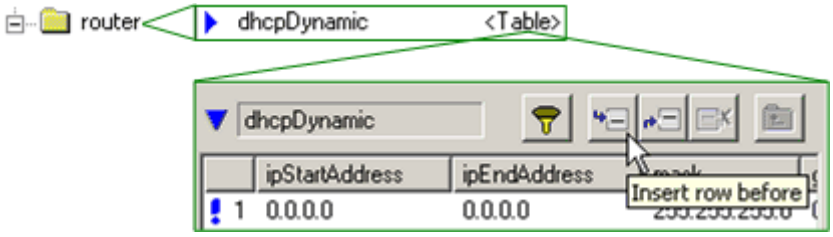
Pour assigner des adresses IP¨à une unité IP, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router, sélectionnez l'attribut dhcpStatic et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour assigner une adresse IP fixe à une unité IP, pour une durée indéterminée. Ajoutez une ligne au tableau dhcpStatic pour chaque adresse IP que vous souhaitez assigner.
2	Configurez les éléments du tableau dhcpStatic. Les plus importants sont: • ipAddress. Utilisez cet élément pour assigner une adresse IP à un client donné. Ce client sera identifié par son adresse MAC. • mask. Utilisez cet élément pour affecter au client son masque subnet. • gateway. Utilisez cet élément pour définir la passerelle par défaut pour le subnet du client. • macAddress. Utilisez cet élément pour entrer l'adresse MAC du client. Reportez-vous à telindus1421Router/router/dhcpStatic page 91 pour de plus amples informations.

MU-9.1.3 Assignation d'adresses IP dynamiques

Reportez-vous à MU-9.1.1 - Introduction au DHCP page 254 pour la présentation.

Pour assigner des adresses IP dynamiques à une unité IP, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router, sélectionnez l'attribut dhcpStatic et ajoutez une ou plusieurs entrées à ce tableau.  Utilisez cet attribut pour assigner une adresse IP sélectionnée dans une gamme d'adresses IP à une unité IP, pour une durée indéterminée. Ajoutez une ligne au tableau dhcpDynamic pour chaque adresse IP que vous souhaitez créer.
2	Configurez les éléments du tableau dhcpDynamic. Les plus importants sont: • ipStartAddress. Utilisez cet élément pour définir l'adresse de départ de la gamme d'adresses IP. C'est à partir de cette gamme que se fera l'affectation dynamique d'une adresse IP à un client. • ipEndAddress. Utilisez cet élément pour définir l'adresse de fin de la gamme d'adresses IP. C'est à partir de cette gamme que se fera l'affectation dynamique d'une adresse IP à un client. • mask. Utilisez cet élément pour définir le masque subnet d'un client pour la gamme d'adresses IP spécifiée. • gateway. Utilisez cet élément pour définir la passerelle par défaut pour le subnet du client. • leaseTime. Utilisez cet élément pour définir la durée maximale pendant laquelle un client pourra disposer d'une adresse IP à partir de la gamme d'adresses IP spécifiée. Si 00000d 00h 00m 00s (valeur par défaut) est spécifié, la durée de location est illimitée. Reportez-vous à telindus1421Router/router/dhcpDynamic page 92 pour de plus amples informations.

MU-9.1.4 Configuration du Routeur Telindus 1421 SHDSL comme agent relais DHCP

Reportez-vous à MU-9.1.1 - Introduction au DHCP page 254 pour la présentation.

Pour configurer le Routeur Telindus 1421 SHDSL comme agent relais DHCP, procédez de la façon suivante:

Etape	Action
1	Spécifiez (a) la ou les adresses IP de secours en utilisant l'élément helpers dans la structure ip. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour de plus amples informations.
2	Spécifiez ensuite le protocole de secours. Par défaut, le tableau helperProtocols est vide. Dans ce cas, les demandes BootP/DHCP (entre autres) sont transmises automatiquement. Toutefois, le fait de spécifier au moins une valeur dans le tableau helperProtocols efface automatiquement la liste des secours par défaut. Dans ce cas, il convient d'entrer explicitement le protocole BootP/DHCP dans le tableau helperProtocols. Reportez-vous à telindus1421Router/router/helperProtocols page 88 pour de plus amples informations.

MU-9.2 Configuration des restrictions d'accès

Cette section explique comment contrôler l'accès au Routeur Telindus 1421 SHDSL pour les données de gestion et d'utilisateurs. Elle donne d'abord un aperçu des différentes restrictions d'accès devant être appliquées au Routeur Telindus 1421 SHDSL. Elle précise ensuite la restriction d'accès la plus complexe: les listes d'accès étendu. Elle présente les listes d'accès étendu et vous indique comment les configurer.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.2.1 - Les différentes restrictions d'accès sur le Routeur Telindus 1421 SHDSL page 259
- MU-9.2.2 - Présentation des listes d'accès étendu page 263
- MU-9.2.3 - Configuration d'une liste d'accès étendu page 264
- MU-9.2.4 - Synchronisation d'une liste d'accès étendu page 266
- MU-9.2.5 - Remarques sur les listes d'accès étendu page 270

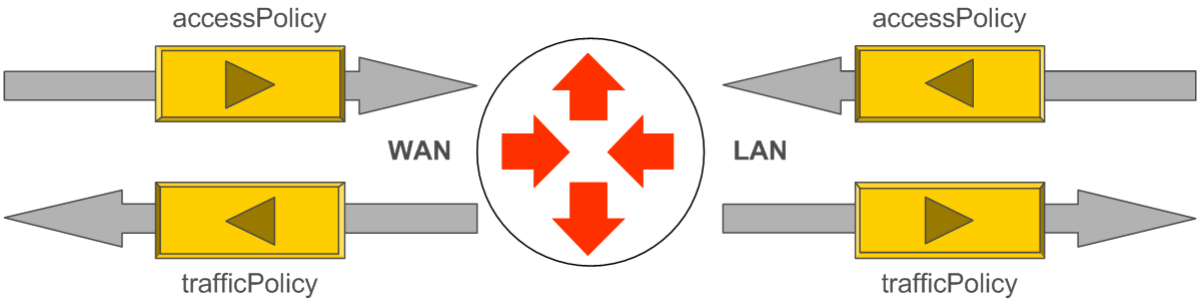
MU-9.2.1 Les différentes restrictions d'accès sur le Routeur Telindus 1421 SHDSL

Cette section donne un aperçu des différentes restrictions d'accès devant être appliquées au Routeur Telindus 1421 SHDSL.

Interface IP

Vous pouvez appliquer les restrictions d'accès suivantes sur une interface IP

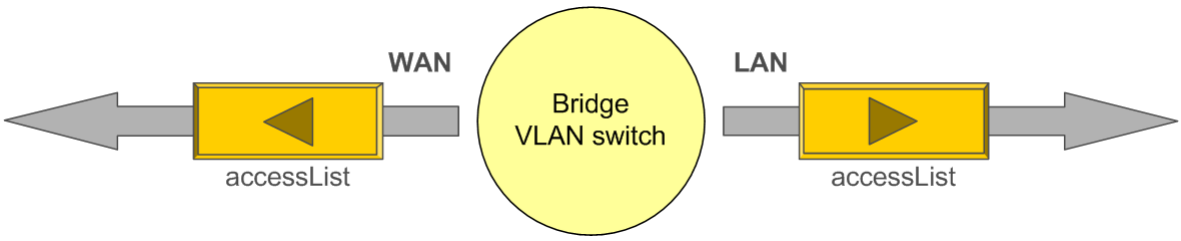
Restrictions d'accès aux données utilisateur	Configuration rapide
Liste d'accès étendu interne avec règles “permettre” et/ou “refuser”.	1. Ajoutez et configurez un objet router/trafficPolicy[ ] , par exemple trafficPolicy[myInList]. 2. Appliquez la politique de trafic en entrant le nom d'indice de l'objet router/trafficPolicy[ ] comme valeur de l'élément accessPolicy dans la structure ip (p ex. “myInList”). Reportez-vous à MU-9.2.3 - Configuration d'une liste d'accès étendu page 264 pour de plus amples informations.
Liste d'accès étendu externe avec règles "permettre".	1. Ajoutez et configurez un objet router/trafficPolicy[ ] , par exemple trafficPolicy[myInList]. 2. Appliquez la politique de trafic en entrant le nom d'indice de l'objet router/trafficPolicy[ ] comme valeur de l'élément accessPolicy dans la structure ip (p ex. “myOutList”). Reportez-vous à MU-9.2.3 - Configuration d'une liste d'accès étendu page 264 pour de plus amples informations.

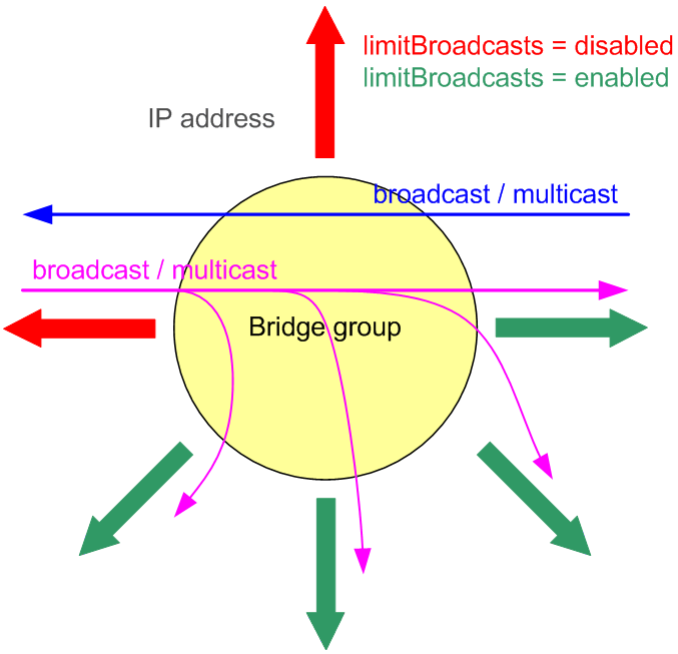


Interface pont

Vous pouvez appliquer les restrictions d'accès suivantes sur une interface pont:

Restrictions d'accès aux données utilisateur	Configuration rapide
Liste d'accès simple externe avec règles "refuser".	1. Ajoutez et configurez un objet bridge/accessList[ ] , par exemple accessList[myList]. 2. Appliquez la liste d'accès en entrant le nom d'indice de l'objet bridge/accessList[ ] comme valeur de l'élément accessList dans la structure bridging (p. ex. “myList”). Reportez-vous à telindus1421Router/bridge/accessList[ ]/macAddress page 153 pour de plus amples informations.
Empêcher les diffusions et les multidiffusions de parvenir à toutes les interfaces	Configurez l'élément limitBroadcasts dans la structure bridging. Reportez-vous à limitBroadcasts page 246 pour de plus amples informations.

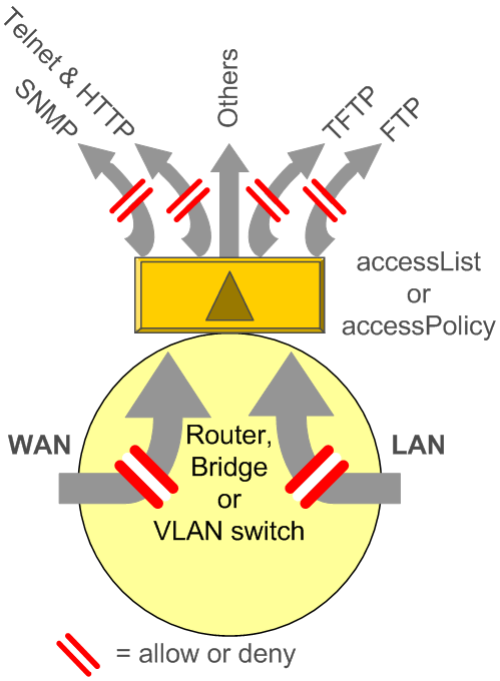




Pile de protocoles

Vous pouvez appliquer les restrictions d'accès suivantes sur la pile de protocoles:

Restrictions d'accès aux données de gestion	Configuration rapide
Liste d'accès simple interne avec règles “permettre” et/ou “refuser”.	Configurez l'attribut accessList dans l'objet management . Reportez-vous à telindus1421Router/management/accessList page 163 pour de plus amples informations.
Liste d'accès étendu interne avec règles “permettre” et/ou “refuser”.	1. Ajoutez et configurez un objet router/trafficPolicy[ ] , par exemple trafficPolicy[myMgtList]. 2. Appliquez la politique de trafic en entrant le nom d'indice de l'objet router/trafficPolicy[ ] comme valeur de l'attribut accessPolicy dans l'objet management (p ex. “myMgtList”). Reportez-vous à MU-9.2.3 - Configuration d'une liste d'accès étendu page 264 pour de plus amples informations.
Restrictions de protocole faciles sans besoin d'une liste d'accès (Telnet, FTP, TFTP, SNMP: permettre / refuser).	Configurez les attributs telnet, ftp, tftp et snmp dans l'objet management . Reportez-vous à MR-1.13 - Management configuration attributes page 158 pour de plus amples informations.
Restrictions d'accès par interface IP (permettre / refuser)	Configurez l'élément mgmtAccess dans la structure ip. Reportez-vous à mgmtAccess page 59 pour de plus amples informations.
Restrictions d'accès par interface pont (au niveau VLAN: permettre / refuser)	Configurez l'attribut localAccess dans l'objet bridgeGroup . Reportez-vous à telindus1421Router/bridge/bridgeGroup/localAccess page 148 pour de plus amples informations.


Telnet & HTTP
SNMP
Others
TFTP
FTP
accessList
or
accessPolicy
WAN
Router,
Bridge
or
VLAN switch
LAN
= allow or deny

MU-9.2.2 Présentation des listes d'accès étendu

Qu'est-ce qu'une liste d'accès étendu?

Les listes d'accès contrôlent l'accès vers ou en provenance d'un certain nombre de services spécifiques ou d'adresses IP. Une liste d'accès décrit les conditions dans lesquelles il est possible de les transmettre (permettre) ou de ne pas les transmettre (refuser).

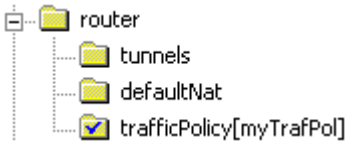
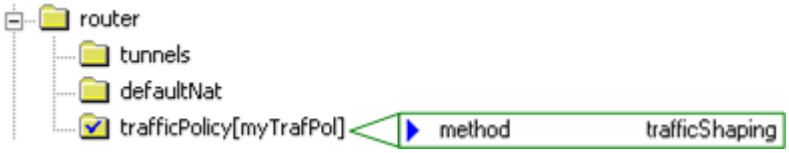
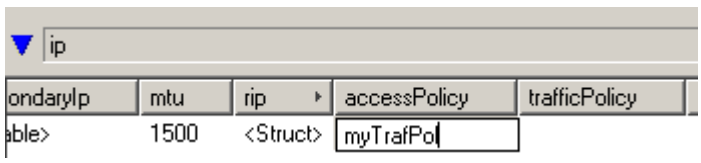
Lorsque les listes d'accès sont combinées avec une translation NAT/PAT, les conditions de la liste sont appliquées avant que la translation NAT/PAT ne soit effectuée.

Sur le Routeur Telindus 1421 SHDSL, les listes d'accès étendu sont mises en œuvre en utilisant la fonction de politique de trafic et en définissant les règles de configuration de trafic.

MU-9.2.3 Configuration d'une liste d'accès étendu

Cette section explique comment configurer une liste d'accès étendu. MU-9.2.4 - Synchronisation d'une liste d'accès étendu page 266 explique comment configurer la liste d'accès, c'est-à-dire comment définir les critères de filtrage.

Pour configurer une liste d'accès étendu, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et ajoutez un objet trafficPolicy[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43).  P. ex. trafficPolicy[myTrafPol]
2	Dans l'objet trafficPolicy[ ] que vous venez de créer, assurez-vous que la méthode d'attribut de configuration est réglée sur trafficShaping (valeur par défaut). 
3	Configurez l'attribut de configuration telindus1421Router/router/trafficPolicy[ ]/trafficShaping pour adapter vos critères de filtrage. Reportez-vous à MU-9.2.4 - Synchronisation d'une liste d'accès étendu page 266.
4	Appliquez la politique de trafic à l'interface souhaitée. Voir ci-dessous. **Configuration d'une liste d'accès étendu interne sur une interface IP** 1. Allez à l'attribut ip de l'interface sur laquelle vous souhaitez appliquer votre liste d'accès étendu. Par exemple, supposons que vous souhaitiez appliquer une liste d'accès étendu à l'interface LAN. Allez alors à l'objet lanInterface puis à l'attribut ip. 2. Dans l'attribut ip, entrez le nom d'indice de l'objet trafficPolicy[ ] que vous avez créé à l'étape 1 comme valeur de l'élément accessPolicy. Dans notre exemple, entrez la chaîne myTrafPol comme valeur de l'élément accessPolicy. 

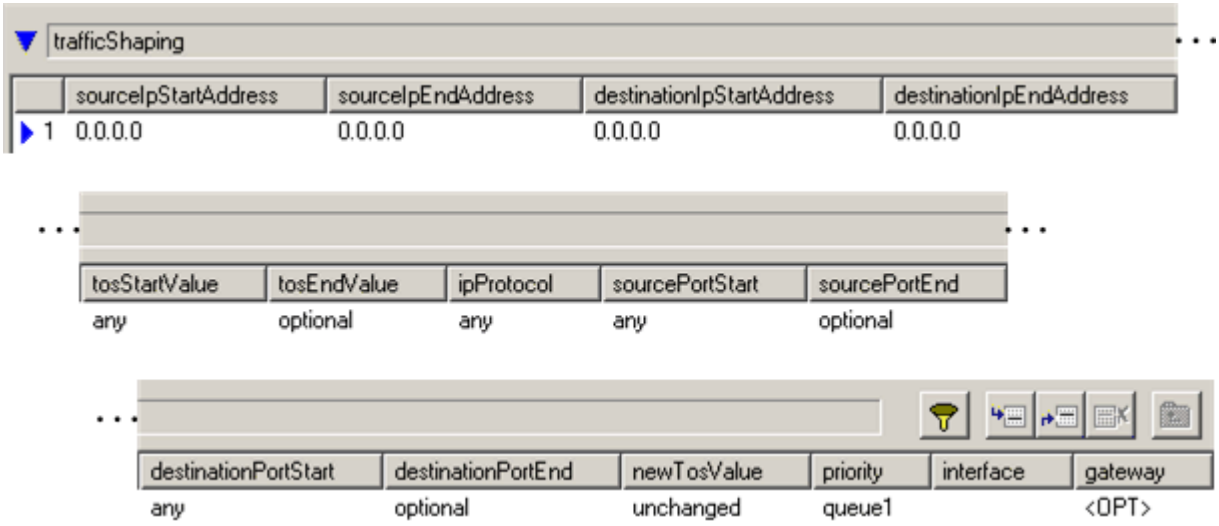
Etape	Action
5	**Configuration d'une liste d'accès étendu externe sur une interface IP** 1. Allez à l'attribut ip de l'interface sur laquelle vous souhaitez appliquer votre liste d'accès étendu. Par exemple, supposons que vous souhaitiez appliquer une liste d'accès étendu à l'interface LAN. Allez alors à l'objet lanInterface puis à l'attribut ip. 2. Dans l'attribut ip, entrez le nom d'indice de l'objet trafficPolicy[ ] que vous avez créé à l'étape 1 comme valeur de l'élément trafficPolicy. Dans notre exemple, entrez la chaîne myTrafPol comme valeur de l'élément trafficPolicy.
6	**Configuration d'une liste d'accès étendu interne sur la pile de protocoles** Allez à l'objet management et entrez le nom d'indice de l'objet trafficPolicy[ ] que vous avez créé à l'étape 1 comme valeur de l'attribut accessPolicy. **Remarque importante** Il est possible que le Routeur Telindus 1421 SHDSL doive répondre à des demandes DHCP ou terminer les tunnels L2TP et IPSec. Dans ce cas, si vous avez défini une liste d'accès sur la pile de protocoles, assurez-vous que ces protocoles peuvent accéder à la pile.

MU-9.2.4 Synchronisation d'une liste d'accès étendu

Alors que MU-9.2.3 - Configuration d'une liste d'accès étendu page 264 vous indique comment configurer une liste d'accès étendu, cette section vous montre comment synchroniser la liste d'accès, c'est-à-dire comment définir les critères de filtrage.

Vous devez définir les critères de filtrage dans l'attribut telindus1421Router/router/trafficPolicy[ ]/trafficShaping. Il s'agit là d'un tableau qui est vide par défaut, mais auquel vous pouvez ajouter plusieurs lignes (entrées).

La figure qui suit montre une vue du tableau trafficShaping contenant une seule ligne:



Comme vous pouvez le voir à partir des éléments de ce tableau trafficShaping, vous pouvez définir le filtrage en fonction de plusieurs critères:

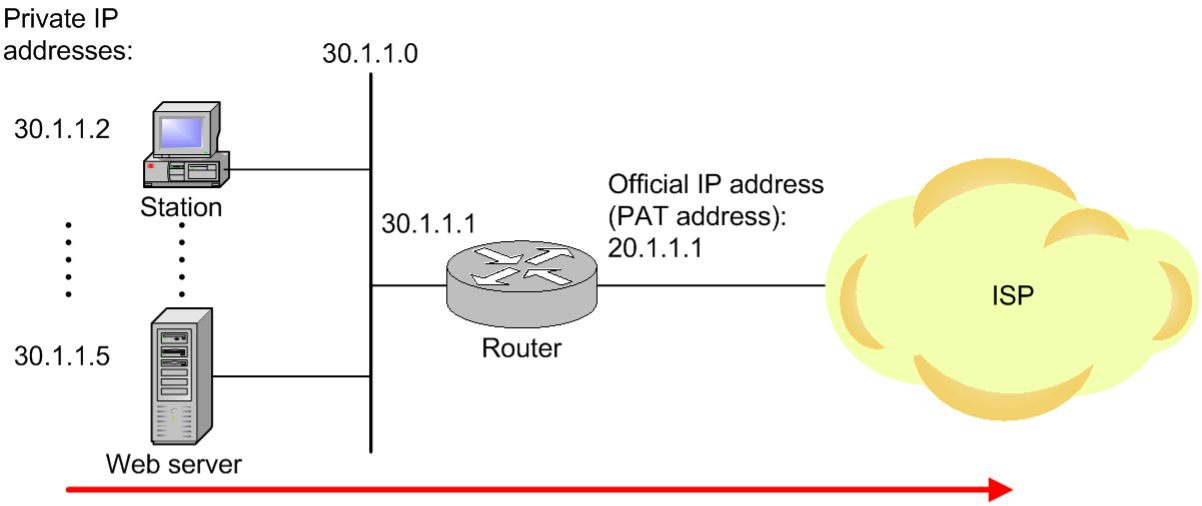
critère de filtrage	Description
adresses IP	• 1 adresse IP entrez une adresse IP dans l'élément sourceIpStartAddress et/ou destinationIpStartAddress. • Gamme d'adresses IP: entrez une gamme d'adresses IP en utilisant les éléments … - sourceIpStartAddress et sourceIpEndAddress and/or - destinationIpStartAddress et destinationIpEndAddress Ainsi, si vous avez défini une ou plusieurs adresses IP dans le taleau trafficShaping, le trafic en provenance (source) ou vers (destination) ces adresses IP est autorisé. Tous les autres trafics sont refusés.
protocole IP	Spécifiez un protocole IP en utilisant l'élément ipProtocol. Sélectionnez l'un des protocoles IP commun dans la boîte déroulante de l'élément ipProtocol, ou entrez directement un numéro de protocole particulier dans le champ d'élément ipProtocol. Ainsi, si vous définissez un protocole IP dans le tableau trafficShaping, le trafic comportant ce protocole IP est autorisé. Tous les autres trafics sont refusés.

critère de filtrage	**Description**
numéro de port	• 1 numéro de port: entrez un numéro de port dans l'élément sourcePortStart et/ou destinationPortStart. • gamme de numéros de port: entrez une gamme de numéros de port en utilisant les éléments… - sourcePortStart et sourcePortEnd and/or - destinationPortStart et destinationPortEnd Ainsi, si vous définissez un ou plusieurs numéros de port dans le tableau trafficShaping, le trafic comportant ces numéros de port est autorisé. Tous les autres trafics sont refusés. Le filtrage par les seuls numéros de port n'est pas possible. De plus, vous ne pouvez filtrer par numéros de port que si le protocole IP est réglé sur TCP ou UDP. En d'autres termes, si l'élément du protocole IP est réglé sur une valeur autre que TCP ou UDP, tous les éléments de port sont ignorés.
valeur Type Of Service (TOS)	• 1 valeur TOS: entrez une valeur TOS dans l'élément tosStartValue. • gamme de valeurs TOS: entrez une gamme de valeurs TOS en utilisant les éléments tosStartValue et tosEndValue. Ainsi, si vous définissez une ou plusieurs valeurs TOS dans le tableau trafficShaping, le trafic comportant ces valeurs TOS est autorisé. Tous les autres trafics sont refusés.

Exemple - configuration d'une liste d'accès étendu

Il s'agit ici d'un exemple de réseau connecté à l'internet et pour lequel les conditions suivantes sont nécessaires:

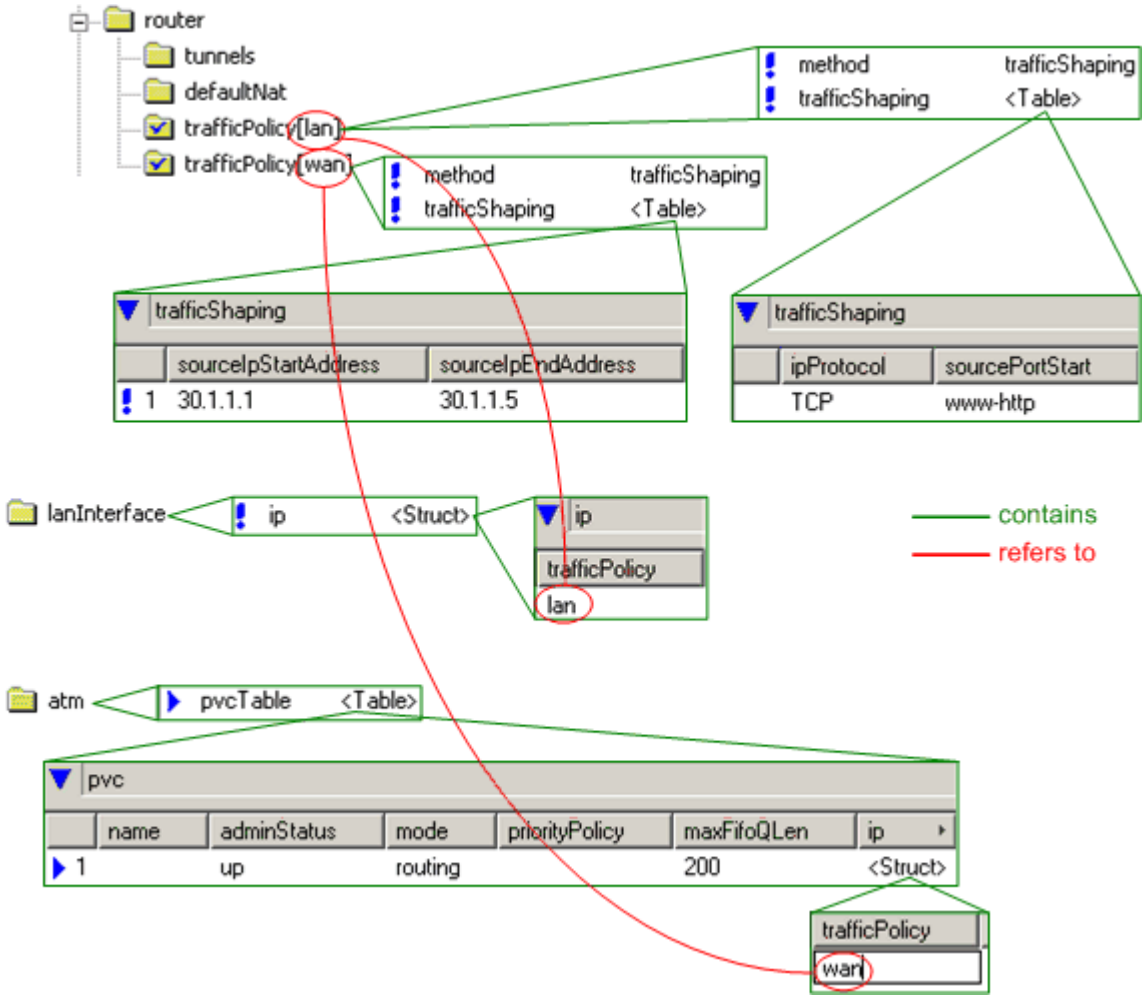
- seules 5 stations peuvent avoir accès à l'internet.
- seul le port HTTP pour la navigation sur le web est ouvert pour les paquets entrants provenant de l'internet.



The access list on the WAN interface (refer to the trafficPolicy[wan] object) filters outgoing traffic. Only the stations with IP addresses 30.1.1.1 up to 30.1.1.5 are allowed to access the Internet.	PAT : the source IP address 30.1.1.x is changed to 20.1.1.1 and the source port is changed to a free port.	To the WAN interface.

To the LAN interface.	The access list on the LAN interface (refer to the trafficPolicy[lan] object) filters incoming traffic. Only port number 80 (www-http) is allowed.

La figure qui suit montre comment configurer les listes d'accès étendu:



MU-9.2.5 Remarques sur les listes d'accès étendu

- Par défaut, les entrées dans le tableau trafficShaping sont les règles “permettre”, c'est-à-dire que seul le trafic défini dans le tableau est autorisé, tous les autres trafics sont rejetés (indépendamment du fait que le tableau de configuration du trafic est utilisé comme une liste d'accès, pour la politique de priorité ou pour l'acheminement en fonction de la politique). Toutefois, vous pouvez inverser une entrée en en faisant une règle “refuser" en entrant “discard” comme valeur de l'élément interface.

- Si plus d'une seule entrée s'applique à un même paquet, choisissez alors l'entrée qui dispose de la gamme de filtre la plus étroite (lorsque l'on considère les critères de filtrage de la gauche vers la droite). Par exemple: deux rangées de la table trafficShaping s'appliquent au même paquet, mais la rangée 1 souhaite envoyer des paquets à la file 3 et la rangée 2 transmettre des paquets à la file de longue attente. Dans ce cas, c'est l'adresse de la source IP qui est d'abord prise en compte. La rangée présentant la plus petite gamme l'emporte. Si les gammes sont exactement les mêmes, l'adresse de la destination IP est alors prise en compte. Et ainsi de suite. Si les deux rangées sont parfaitement identiques à l'exception de la file d'attente, l'une des rangées est choisie de manière aléatoire.

- Vous ne devez pas nécessairement compléter les adresses IP dans la table trafficShaping. Il est parfaitement valable de filtrer les protocoles IP, la combinaison protocole IP/port ou les valeurs TOS uniquement. Le filtrage par les seuls numéros de port n'est pas possible. De plus, vous ne pouvez filtrer par numéros de port que si le protocole IP est réglé sur TCP ou UDP. En d'autres termes, si l'élément du protocole IP est réglé sur une valeur autre que TCP ou UDP, tous les éléments de port sont ignorés.

MU-9.3 Configurer les VLAN

Cette section présente les VLAN et fournit une description rapide des attributs que vous pouvez utiliser pour configurer les VLAN.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.3.1 - Introduction aux VLAN page 272
- MU-9.3.2 - Configuration d'un VLAN page 273
- MU-9.3.3 - Configuration de la commutation VLAN page 275

MU-9.3.1 Introduction aux VLAN

Remarque importante

Vous ne pouvez pas créer des VLAN sur l'interface LAN et effectuer une commutation VLAN (reportez-vous à MU-9.3.3 - Configuration de la commutation VLAN page 275) en même temps. Ainsi, choisissez, soit de créer des VLAN sur l'interface LAN, soit de procéder à la commutation VLAN.

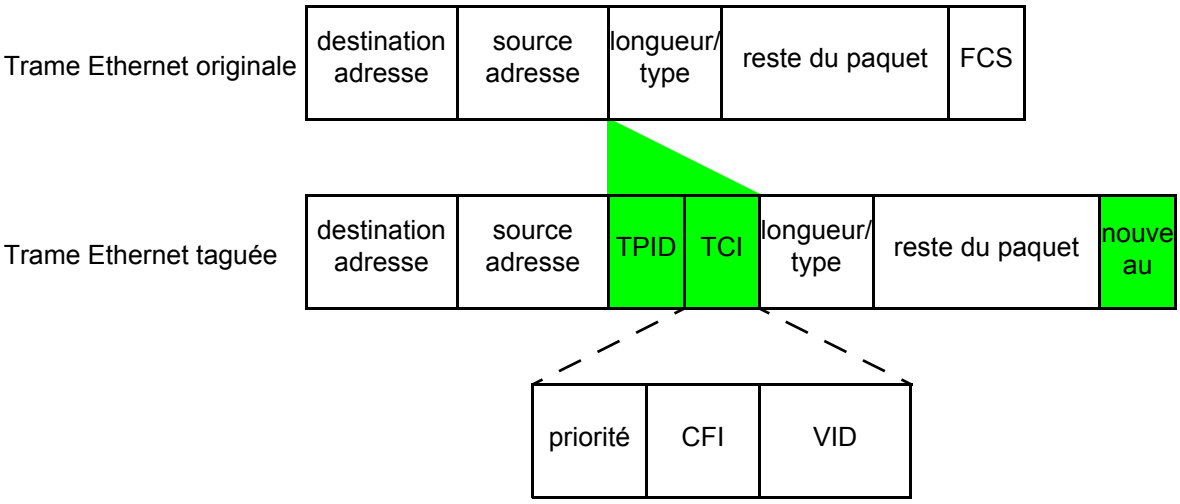
Qu'est-ce qu'un VLAN?

Un Virtual LAN (VLAN) est un groupe d'unités présentes sur un ou plusieurs LAN configurées (à l'aide du logiciel de gestion) de telle manière qu'elles puissent communiquer comme si elles étaient raccordées au même câble, alors qu'elles sont, en fait, situées sur plusieurs segments LAN différents. Les VLAN étant basés sur des connexions logiques plutôt que physiques, ils sont extrêmement flexibles.

Qu'est-ce qu'un tag VLAN?

L'en-tête de tag VLAN est insérée immédiatement après les champs d'adresse MAC de destination et d'adresse MAC source de la trame. L'en-tête tag VLAN se divise en deux parties:

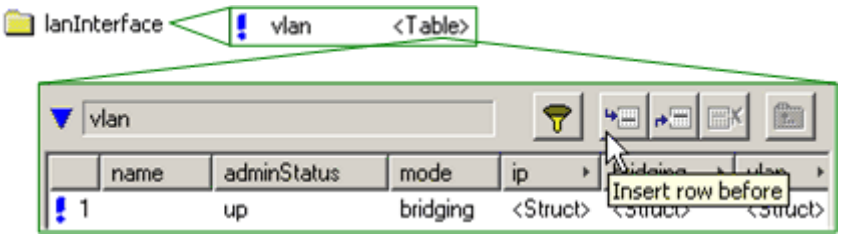
- TPID (Tag Protocol Identifier). Le TPID à encodage 802.1Q Ethernet est défini sous la forme de deux octets avec la valeur “8100”.
- TCI (Tag Control Information). Le champ TCI a également une longueur de deux octets et contient:
  - la priorité utilisateur . Les bits de priorité utilisateur représentent huit niveaux de priorité, 0 à 7. IEEE 802.1P définit le fonctionnement de ces trois bits de priorité.
  - CFI (Canonical Format Indicator). Le bit CFI indique que l'ensemble des informations d'adresse MAC transmises par la trame et pouvant être présentes dans les données MAC sont en format Canonical.
  - VID (VLAN Identifier). Le champ VID à douze bits identifie le VLAN auquel appartient la trame. Trois valeurs VID sont réservées par la norme 802.1Q.



MU-9.3.2 Configuration d'un VLAN

Reportez-vous à MU-9.3.1 - Introduction aux VLAN page 272 pour la présentation.

Pour créer un VLAN, procédez de la façon suivante:

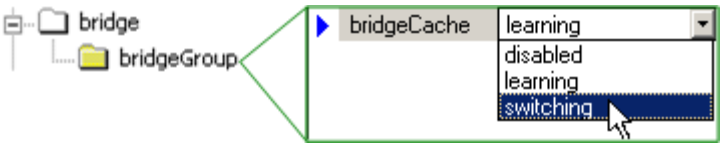
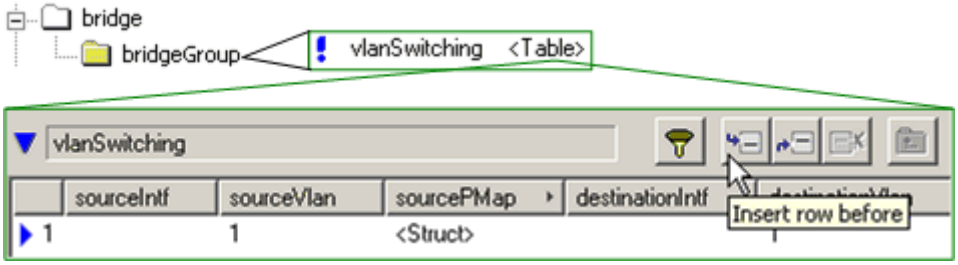
Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet lanInterface, sélectionnez l'attribut vlan et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour configurer les VLAN souhaités. Ajoutez une ligne au tableau vlan pour chaque VLAN que vous souhaitez configurer. Tant qu'aucun VLAN n'est créé dans la table vlan, l'interface LAN accepte à la fois les trames de VLAN non tagués et de VLAN tagués. Les trames VLAN *untagged* sont pontées et/ou acheminées (en fonction du réglage de l'attribut mode). Les trames VLAN *tagged* sont pontées (si l'attribut mode est réglé sur bridging ou bridgingAndRouting, sinon elles sont rejetées). Dès qu'un VLAN est créé dans la table vlan, l'interface LAN accepte encore les trames non taguées VLAN mais n'accepte que celles des trames taguées VLAN dont le VLAN ID correspond au VLAN ID configuré dans la table vlan (voir l'élément vid ci-dessous). Les autres trames taguées VLAN sont refusées.
2	Configurez les éléments du tableau vlan. • name. Utilisez cet élément pour assigner un nom administratif au VLAN. • adminStatus. Utilisez cet élément pour activer ou désactiver le VLAN. • mode. Utilisez cet élément pour déterminer si, pour le VLAN correspondant, des paquets IP sont traités par l'acheminement ou le pontage. • ip. Utilisez cet élément pour configurer les paramètres de l'IP du VLAN. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour de plus amples informations. • bridging. Utilisez cet élément pour configurer les paramètres de pontage si l'attribut mode est défini sur bridging. Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 pour de plus amples informations. • vlan. Utilisez cet élément pour configurer les paramètres spécifiques du VLAN. Voir ci-dessous. Reportez-vous à telindus1421Router/lanInterface/vlan page 24 pour de plus amples informations.

Etape	Action
3	Configurez la structure vlan dans la table vlan. Les éléments de cette structure sont: • vid. Utilisez cet élément pour définir l'ID du VLAN. • tagSignificance. Utilisez cet élément pour déterminer si le tag VLAN a une signification locale ou globale. Cet élément est uniquement pertinent lorsque vous définissez l'élément mode sur bridging. Si tagSignificance est réglé sur … - local, l'en-tête du VLAN ne concerne que le VLAN lui-même. Lors de la réception d'un paquet sur le VLAN, l'en-tête du VLAN est barrée avant que le paquet ne soit transmis au moteur de pontage. Lors de la transmission d'un paquet sur le VLAN, l'en-tête du VLAN est insérée. - global, l'en-tête du VLAN n'est pas modifiée lors de la transmission des paquets. Lors de la connexion de deux ou plusieurs VLAN Ethernet au même groupe de pontage, assurez-vous d'avoir réglé tagSignificance sur local, car les deux VLAN utilisent des ID différentes. Reportez-vous à telindus1421Router/lanInterface/vlan/vlan page 26 pour de plus amples informations.

MU-9.3.3 Configuration de la commutation VLAN

Reportez-vous à MU-9.3.1 - Introduction aux VLAN page 272 pour une introduction aux VLAN.

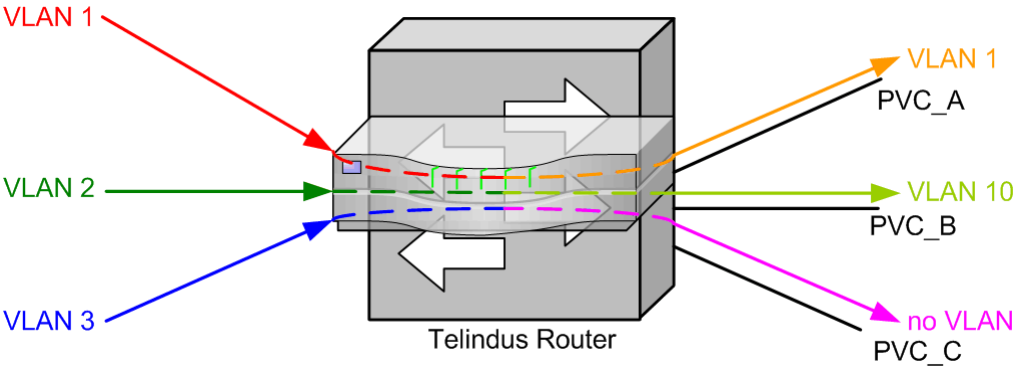
Pour configurer la commutation VLAN, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet bridge/bridgeGroup et réglez l'attribut bridgeCache sur switching. 
2	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet bridge/bridgeGroup, sélectionnez l'attribut vlanSwitching et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour spécifier quels VLAN vous souhaitez commuter. Ajoutez une ligne au tableau vlanSwitching pour chaque VLAN que vous souhaitez commuter.

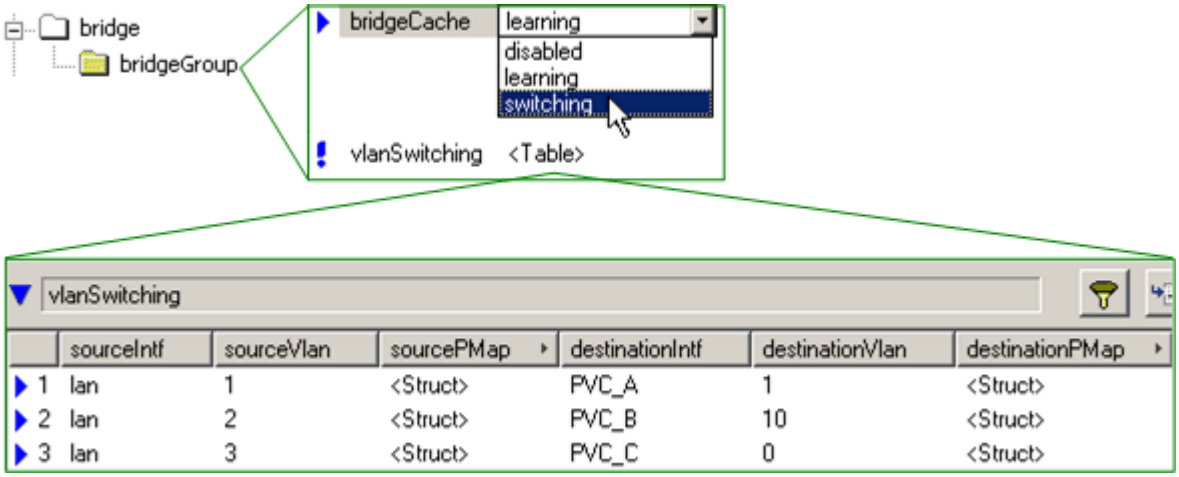
Etape	Action
3	Configurez les éléments du tableau vlanSwitching: • sourceIntf. Utilisez cet élément pour entrer le nom de l'interface de source (physique) qui transporte le VLAN qui doit être commuté. • sourceVlan. Utilisez cet élément pour entrer l'ID du VLAN qui doit être commuté. Entrer 0 comme ID du VLAN efface le tag du VLAN de la trame Ethernet. • sourcePMap. Utilisez cet élément pour redéfinir les priorités VLAN, si vous le souhaitez. La commutation étant bidirectionnelle, vous pouvez redéfinir les priorités pour les deux directions (c'est-à-dire à l'interface “source” et “destination”). • destinationIntf. Utilisez cet élément pour entrer le nom de l'interface de destination (physique) qui transporte le VLAN qui a été commuté. L'interface de destination peut également être un groupe de pontage, auquel cas il vous suffit d'entrer le nom de ce groupe. • destinationVlan. Utilisez cet élément pour entrer l'ID du VLAN une fois commuté. Entrer 0 comme ID du VLAN efface le tag du VLAN de la trame Ethernet. • destinationPMap. Utilisez cet élément pour redéfinir les priorités VLAN, si vous le souhaitez. La commutation étant bidirectionnelle, vous pouvez redéfinir les priorités pour les deux directions (c'est-à-dire à l'interface “source” et “destination”). **Remarques importantes** •Notez qu'une ligne de la table vlanSwitching représente une connexion bidirectionnelle, c'est-à-dire que les données sont commutées de la source à la destination, et vice versa. • Notez aussi que les connexions point à point sont possibles. Les connexions point à multipoints ne sont pas possibles. En d'autres termes, un VLAN ne peut apparaître qu'une fois dans la table vlanSwitching. Reportez-vous à telindus1421Router/bridge/bridgeGroup/vlanSwitching page 150 pour de plus amples informations sur les éléments de l'attribut de configuration vlanSwitching.

Exemple – configuration de commutation VLAN

La figure qui suit montre l'interface VLAN comportant 3 VLAN commutés sur 3 cartes ATM différentes. L'une des ID VLAN est conservée, l'autre est modifiée, la troisième barrée.



La figure qui suit montre comment configurer le groupe de pontage pour la commutation VLAN.



MU-9.4 Configuration de tunnels L2TP

Cette section présente le Layer 2 Tunnelling Protocol (L2TP) et donne une rapide description des attributs utilisables pour sa configuration.

Le tableau suivant donne un aperçu de ce chapitre:

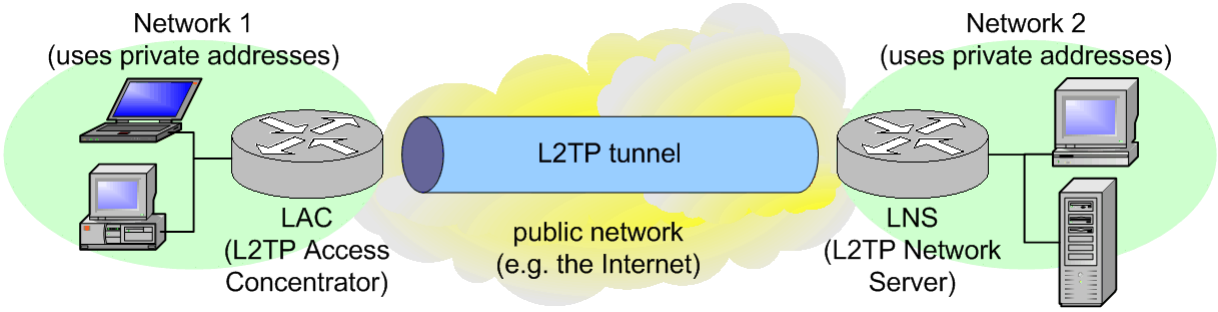
- MU-9.4.1 - Présentation des tunnels L2TP page 279
- MU-9.4.2 - Configuration d'un tunnel L2TP page 281
- MU-9.4.3 - Comment fonctionne un tunnel L2TP? page 284

MU-9.4.1 Présentation des tunnels L2TP

Qu'est-ce qu'un tunnel L2TP?

Le Layer 2 Tunnelling Protocol (L2TP) est un protocole utilisé pour connecter des VPN (Virtual Private Networks) par l'intermédiaire de lignes publiques. Plus spécifiquement, il vous permet de configurer des connexions PPP virtuelles. En d'autres termes, un tunnel L2TP simule une interface PPP supplémentaire qui connecte directement deux routeurs entre eux.

Concrètement, en utilisant le Layer 2 Tunnelling Protocol, vous pouvez connecter plusieurs réseaux locaux privés et physiquement distants les uns aux autres par l'intermédiaire de lignes publiques (telles que l'internet) afin de créer un grand réseau local (virtuel). Et cela sans qu'il soit besoin d'une translation d'adresses.



Terminologie de tunnel L2TP

Le tableau qui suit donne quelques-uns des termes spécifiques au L2TP:

Terme	Description
L2TP Access Concentrator (LAC)	Nœud A agissant comme une extrémité d'un tunnel L2TP. C'est l'équivalent du L2TP Network Server (LNS). Les paquets envoyés du LAC au LNS nécessitent la mise en tunnel par le protocole L2TP.
L2TP Network Server (LNS)	Nœud A agissant comme une extrémité d'un tunnel L2TP. C'est l'équivalent du L2TP Access Concentrator Server (LAC). Le LNS est le point de terminaison logique d'une session PPP mise en tunnel à partir du système distant par le LAC.
Tunnel	Un tunnel existe entre la paire LAC-LNS. Le tunnel se compose d'une connexion de commande et de zéro ou plusieurs sessions L2TP. Ce tunnel transporte les datagrammes PPP encapsulés et les messages de commande entre le LAC et le LNS.
Connexion de commande	Une connexion de commande fonctionne dans la bande sur un tunnel pour contrôler la mise en place, la libération et la maintenance des sessions et du tunnel lui-même.
Messages de commande	Les messages de commande sont échangés entre les paires LAC et LNS, et fonctionnent dans la bande à l'intérieur du protocole du tunnel. Les messages de commande concernent l'aspect du tunnel et des sessions au sein de celui-ci.

Encapsulation de tunnel L2TP

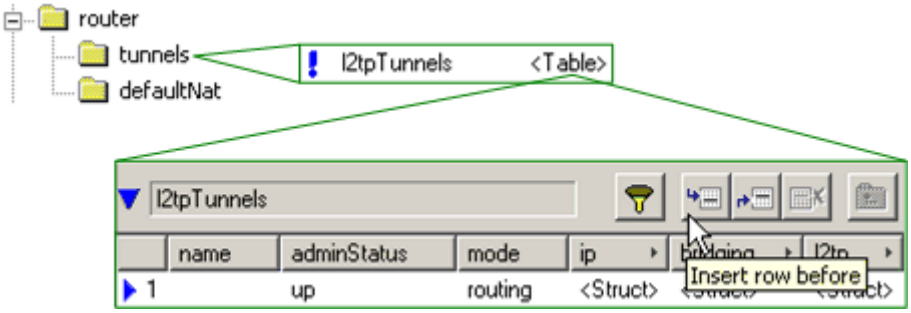
Le tableau qui suit illustre l'encapsulation L2TP des l'interface LAN et WAN:

<table>
<tr><th>Interface</th><th>encapsulation L2TP</th></tr>
<tr><td>Interface WAN</td><td>L'encapsulation L2TP sur l'interface WAN est la suivante:
<table>
<tr><td>PPP
FR
AAL5</td><td>IP</td><td>UDP</td><td>L2TP</td><td>PPP</td><td>IP
Ethernet</td><td>…</td></tr>
</table></td></tr>
<tr><td>Interface LAN</td><td>L'encapsulation L2TP sur l'interface LAN est la suivante:
<table>
<tr><td>MAC</td><td>IP</td><td>UDP</td><td>L2TP</td><td>PPP</td><td>IP
Ethernet</td><td>…</td></tr>
</table></td></tr>
</table>

MU-9.4.2 Configuration d'un tunnel L2TP

Reportez-vous à MU-9.4.1 - Présentation des tunnels L2TP page 279 pour la présentation.

Pour configurer un tunnel L2TP, procédez de la façon suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router/tunnels, sélectionnez l'attribut l2tpTunnels et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour configurer les tunnels Layer 2 Tunnelling Protocol que vous souhaitez configurer. Ajoutez une ligne au tableau 12tpTunnels pour chaque tunnel L2TP que vous souhaitez configurer.
2	Configurez les éléments du tableau 12tpTunnels: • name. Utilisez cet élément pour assigner un nom administratif au tunnel. • adminStatus. Utilisez cet élément pour activer ou désactiver le tunnel. • mode. Utilisez cet élément pour déterminer si, pour l'IP tunnel correspondant, des paquets IP sont traités par le processus d'acheminement, de pontage ou les deux. • ip. Utilisez cet élément pour configurer les paramètres de l'IP du tunnel. La formation d'un tunnel L2TP est basée sur des interfaces logiques. Ces interfaces logiques ont leur propre adresse IP. Reportez-vous à MU-5.2.3 - Explication de la structure ip page 55 pour de plus amples informations. • bridging. Utilisez cet élément pour configurer les paramètres de pontage si l'attribut mode est réglé sur bridging ou routingAndBridging. Reportez-vous à MU-8.2.6 - Explication de la structure bridging page 243 pour de plus amples informations. • l2tp. Utilisez cet élément pour configurer les paramètres L2TP du tunnel. Voir ci-dessous. Reportez-vous à telindus1421Router/router/tunnels/l2tpTunnels page 103 pour de plus amples informations.

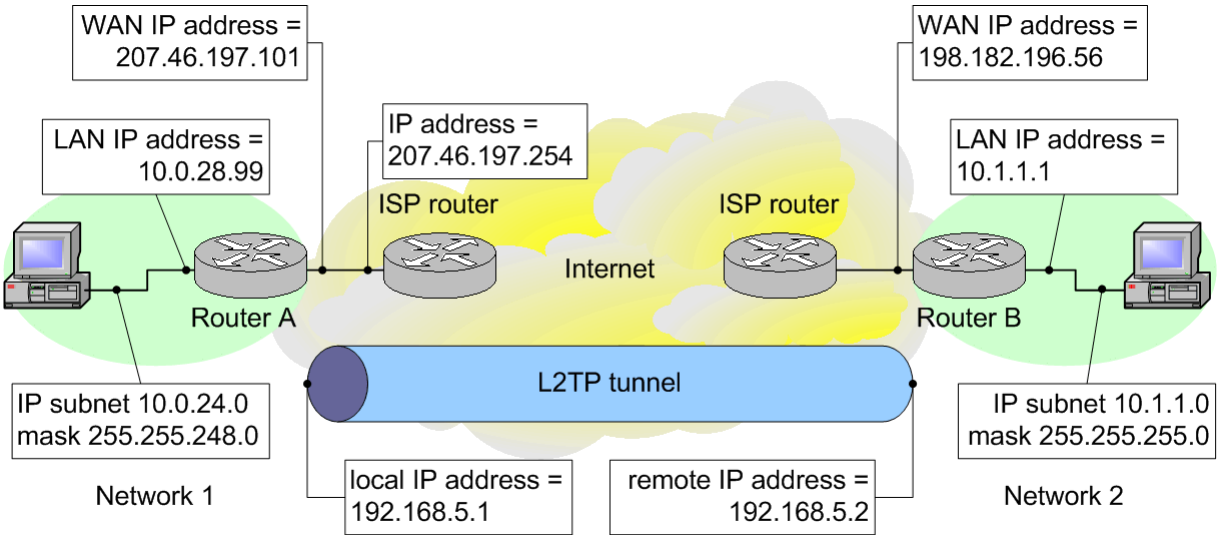
Etape	Action
3	Configurez la structure l2tp dans la table l2tpTunnels. Les éléments les plus importants de cette structure sont: • localIpAddress. Utilisez cet élément pour définir l'adresse IP servant de point de départ du tunnel L2TP. • remoteIpAddress. Utilisez cet élément pour définir l'adresse IP servant de point d'arrivée du tunnel L2TP. • type. Utilisez cet élément pour spécifier le type de tunnel (entrant ou sortant). • mode. Utilisez cet élément pour définir le mode L2TP du Routeur Telindus 1421 SHDSL (LAC, LNS ou auto). Utilisez uniquement auto si un routeur Telindus est situé *des deux côtés* du tunnel. Reportez-vous à telindus1421Router/router/tunnels/l2tpTunnels/l2tp page 104 pour de plus amples informations.

Remarques

- Les tunnels L2TP peuvent également être configurés par le biais d'un hôte IP. Le Routeur Telindus 1421 SHDSL est transparent pour les tunnels configurés par un hôte.
- Des tunnels L2TP multiples sont possibles sur une liaison unique. Actuellement, une seule session PPP est possible par tunnel L2TP.

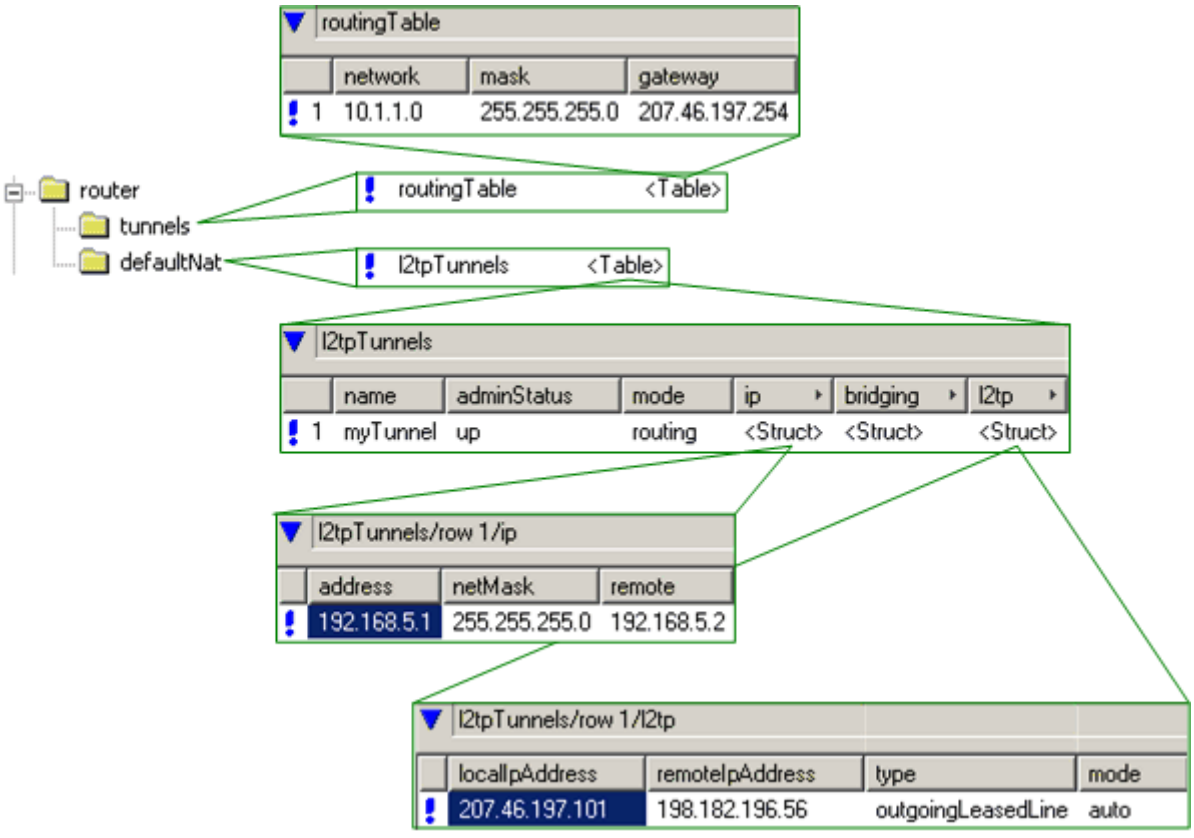
Exemple – configuration d'un tunnel L2TP

Supposons que le réseau privé 1 doive être interconnecté au réseau privé 2 par le biais de l'internet. Pour ce faire, vous souhaitez confitgurer un tunnel L2TP entre les deux routeurs d'accès de ces réseaux privés.



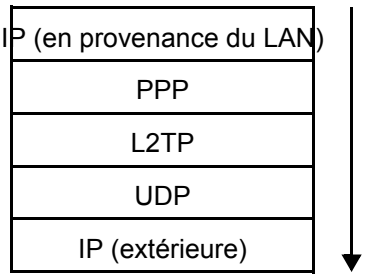
Créer d'abord un chemin entre les interfaces WAN des routeurs A et B. Ensuite, configurez le tunnel entre les interfaces WAN de ces routeurs (le point de départ du tunnel est l'adresse IP 207.46.197.101, le point d'arrivée du tunnel est l'adresse IP 198.182.196.56).

La figure qui suit montre comment configurer le tunnel L2TP:



MU-9.4.3 Comment fonctionne un tunnel L2TP?

Supposons qu'un paquet provenant du LAN ait une adresse de destination pour un réseau accessible par l'intermédiaire d'un tunnel L2TP. Il se produit alors la chose suivante:

Phase	Description
1	Le paquet passe par le processus de décision d'acheminement. Si le résultat de cette décision est un acheminement qui utilise l'interface du tunnel, le paquet est encapsulé en PPP, puis L2TP, UDP, et finalement IP. 
2	Le paquet passe ensuite une nouvelle fois par le processus de décision d'acheminement. Cette fois, en utilisant l'en-tête IP extérieure.
3	Le paquet est acheminé sur l'internet en utilisant l'en-tête IP extérieure.
4	Le paquet est reçu au point de destination du tunnel, où il est ensuite acheminé une nouvelle fois en utilisant l'en-tête IP originale.

MU-9.5 Configuration d'une sécurité IP

Cette section présente la sécurité IP (IPSEC) et fournit une description rapide des attributs que vous pouvez utiliser pour configurer l'IPSEC.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.5.1 - Introduction à l'IPSEC page 286
- MU-9.5.2 - Configuration d'un tunnel L2TP sécurisé IPSEC page 288
- MU-9.5.3 - Puce accélératrice de matériel (HWA) page 290

MU-9.5.1 Introduction à l'IPSEC

Qu'est-ce que l'IPSEC?

L'IPSEC (Internet Protocol Security) est un cadre pour un ensemble de protocoles de sécurité au niveau du réseau ou de la couche de traitement de paquets de données d'une communication en réseau. Des approches de sécurité antérieures avaient intégré la sécurité au niveau des applications du modèle de communication. L'IPSEC est déployé en grande partie lors de la mise en œuvre des Virtual Private Networks (VPN). L'un des grands avantages de l'IPSEC est que des dispositions de sécurité peuvent être traitées sans devoir procéder à des changements dans les ordinateurs des différents utilisateurs.

Les services de sécurité IPSEC (ESP et AH)

L'IPSEC offre deux types de services de sécurité:

- Authentication Header (AH), qui permet essentiellement l'authentification de l'émetteur des données. AH n'est pas supporté par le Routeur Telindus 1421 SHDSL.
- Encapsulating Security Payload (ESP), qui est supporté par le Routeur Telindus 1421 SHDSL, permet à la fois l'authentification de l'émetteur et le cryptage des données.

Les informations spécifiques associées à chacun de ces services sont insérées dans le paquet dans une en-tête qui suit l'en-tête du paquet IP.

Les modes IPSEC

L'IPSEC propose deux modes de base: le mode transport ou le mode tunnel. Le Routeur Telindus 1421 SHDSL supporte actuellement le mode transport L2TP. Le trafic destiné à un tunnel L2TP est sécurisé avec l'IPSEC (voir RFC 3193, sécurisation L2TP en utilisant l'IPSEC).

Qu'est-ce qu'une association de sécurité (SA)?

L'IPSEC propose différentes options de cryptage réseau et d'authentification. Les deux nœuds communiquant doivent déterminer avec exactitude quels algorithmes il convient d'utiliser (p. ex. DES ou 3DES pour le cryptage, MD5 ou SHA pour le contrôle d'intégrité et l'authentification) et doivent partager des codes de sessions.

Toutes ces informations sont décrites dans la Security Association (SA). En d'autres termes, l'association de sécurité est simplement une affirmation de la politique de sécurité négociée entre deux unités.

Il existe deux types d'associations de sécurité:

- Manual SA
- Dynamic SA

Le Routeur Telindus 1421 SHDSL supporte actuellement Manual SA. Il ne nécessite aucune négociation. Toutes les valeurs, y compris les codes, sont fixes et spécifiées dans la configuration. Résultat, chaque pair doit avoir les mêmes options configurées pour que la communication puisse avoir lieu.

En principe, l'association de sécurité est unidirectionnelle (semi-duplex). Cela signifie un SA pour le trafic entrant et un SA pour le trafic sortant. Le Routeur Telindus 1421 SHDSL supporte également le SA en duplex intégral (un SA pour le trafic entrant et sortant à la fois).

Cryptage IPSEC

Avec l'ESP, vous pouvez crypter les données en utilisant la norme de cryptage de données (DES ou 3DES).

DES est une méthode très utilisée de cryptage de données qui utilise un code privé (secret). Comme avec d'autres méthodes cryptographiques à code privé, l'émetteur et le récepteur doivent connaître et utiliser le même code privé. DES applique un code à 56 bits à chaque bloc 64 bits de données. Le triple DES applique trois codes consécutifs.

Authentification IPSEC

Avec l'ESP, vous pouvez non seulement crypter mais aussi authentifier les données, à l'aide de la méthode HMAC (Keyed-Hashing for Message Authentication).

HMAC est un mécanisme d'authentification de message utilisant des fonctions cryptographiques. HMAC peut être utilisé avec n'importe quelle fonction cryptographique itérative, p. ex., MD5, SHA-1, en combinaison avec un code secret partagé.

Qu'est-ce que le Security Parameter Index (SPI)?

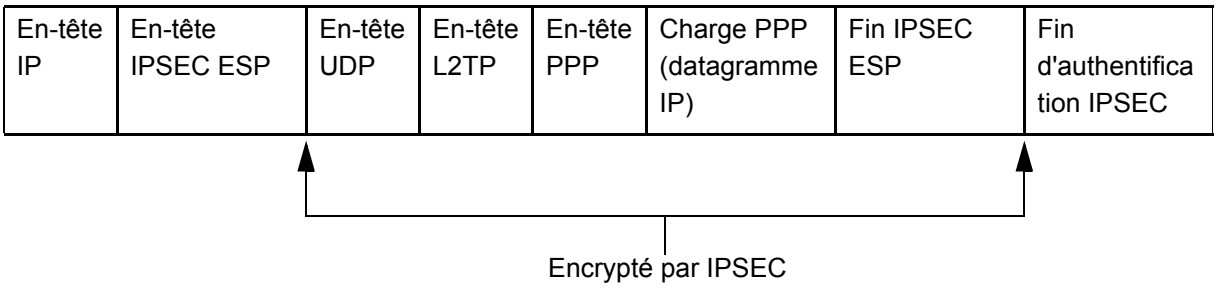
Un SPI est une valeur arbitraire qui identifie uniquement le SA à utiliser dans l'hôte de réception. L'hôte émetteur utilise le SPI pour identifier et sélectionner le SA à utiliser pour sécuriser chaque paquet de données. L'hôte récepteur utilise le SPI pour identifier et sélectionner l'algorithme de cryptage et le code utilisés pour décrypter les paquets de données.

Compatibilité IPSEC

L'IPSEC du Routeur Telindus 1421 SHDSL est compatible avec l'IPSEC utilisé sur les unités Cisco et sur Linux.

Encapsulation IPSEC

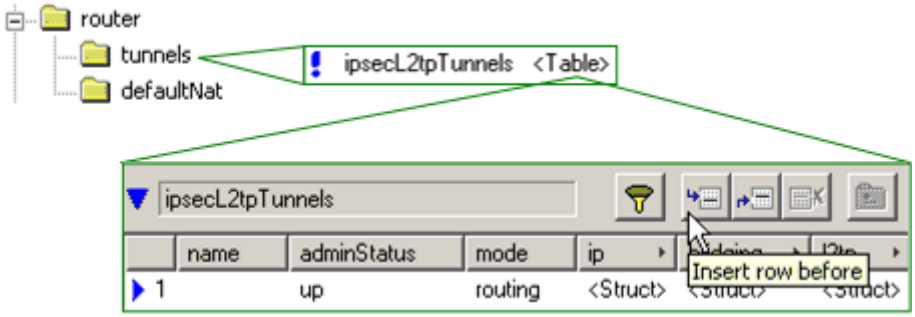
Les points qui suivent illustrent l'encapsulation IPSEC:

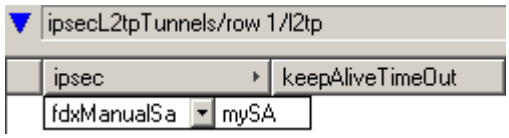


MU-9.5.2 Configuration d'un tunnel L2TP sécurisé IPSEC

Reportez-vous à MU-9.5.1 - Introduction à l'IPSEC page 286 pour la présentation.

Pour configurer un tunnel L2TP sécurisé IPSEC, procédez de la manière suivante:

Etape	Action
1	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et ajoutez un objet manualSA[ ] en dessous (reportez-vous à MU-4.4 - Ajout d'un objet dans l'arborescence page 43). P. ex. manualSA[mySA]
2	Configurez ensuite les attributs de l'objet manualSA[ ] que vous avez ajouté à l'étape 1 en fonction de vos besoins. Ces attributs sont: • espEncryptionAlgorithm. Utilisez cet attribut pour sélectionner l'algorithme qui sera utilisé pour crypter les données lors de l'utilisation de l'IPSEC. • espEncryptionKey. Utilisez cet attribut pour définir le code qui sera utilisé pour le cryptage / décryptage des données lors de l'utilisation de l'IPSEC. • espAuthenticationAlgorithm. Utilisez cet attribut pour sélectionner l'algorithme qui sera utilisé pour authentifier les données lors de l'utilisation de l'IPSEC. • espAuthenticationKey. Utilisez cet attribut pour définir le code qui sera utilisé pour l'authentification lors de l'utilisation de l'IPSEC. • spi. Utilisez cet attribut pour définir la valeur SPI. Chaque association de sécurité doit avoir une valeur SPI unique, car cette valeur est utilisée pour identifier l'association de sécurité. Reportez-vous à MR-1.9.4 - Manual SA configuration attributes page 109 pour de plus amples informations.
3	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router/tunnels, sélectionnez l'attribut ipsecL2tpTunnels et ajoutez une ou plusieurs entrées à cette table.  Utilisez cet attribut pour configurer les tunnels Layer 2 Tunnelling Protocol sécurisés IP que vous souhaitez configurer. Ajoutez une ligne au tableau IpsecL2tpTunnels pour chaque tunnel L2TP IPSEC que vous souhaitez configurer.
4	Configurez les paramètres non IPSEC dans la table ipsecL2tpTunnels décrite dans MU-9.4.2 - Configuration d'un tunnel L2TP page 281. Le seul paramètre lié à l'IPSEC est l'élément ipsec dans la structure l2tp de la table ipsecL2tpTunnels.

Etape	Action
5	Allez à la structure l2tp dans la table ipsecL2tpTunnels et entrez le nom d'indice de l'objet manualSA[ ] que vous avez ajouté à l'étape 1 comme valeur de l'élément ipsec. Ce faisant, vous appliquez l'association de sécurité au tunnel L2TP. Notez que dans l'élément ipsec, vous pouvez choisir entre un SA manuel en semi-duplex ou en duplex intégral (fdxManualSa or hdxManualSa). Reportez-vous à telindus1421Router/router/tunnels/ipsecL2tpTunnels/l2tp/ipsec page 107 pour de plus amples informations. P. ex. dans notre exemple, entrez la chaîne mySA comme valeur de l'élément ipsec. 

MU-9.5.3 Puce accélératrice de matériel (HWA)

Standard Routeur Telindus 1421 SHDSL ou Routeur Telindus 1421 SHDSL HWA

Sur le Routeur Telindus 1421 SHDSL standard, le cryptage dans IPSEC est géré par le logiciel. Cette gestion demandant beaucoup au processeur, les performances de transmission du Routeur Telindus 1421 SHDSL ont tendance à baisser. Par conséquent, le Routeur Telindus 1421 SHDSL existe également en version équipée d'une puce HWA. Cette puce gère le cryptage / décryptage DES et 3DES, soulageant ainsi le logiciel. Cela donne de meilleures performances de transmission.

Comment identifier une version HWA du Routeur Telindus 1421 SHDSL?

Il n'est pas possible de distinguer une version standard d'une version HWA sur son seul aspect extérieur. Cependant, vous pouvez différencier ces deux versions en observant l'attribut d'état telindus1421Router/sysDescr. Si vous êtes équipé d'une version HWA, la chaîne “HWA” ou “3DES” apparaît dans sysDescr.

Exemple:

- Routeur Telindus 1421 SHDSL Txxxx/xxxxx 01/01/00 12:00 indique que vous disposez d'une version standard.
- Routeur Telindus 1421 SHDSL 3DES Txxxx/xxxxx 01/01/00 12:00 indique que vous disposez d'une version 3DES.

Etat de la puce HWA

Lorsque le Routeur Telindus 1421 SHDSL s'initialise, il vérifie la présence de la puce HWA et effectue un test de diagnostic. Si ce test échoue (p. ex. par suite d'une défaillance de la puce HWA), les messages suivants apparaissent dans l'attribut d'état telindus1421Router/messages:

- encryption chip init failed
- encryption chip diag failed

Si la puce HWA est défectueuse, le cryptage DES et 3DES est effectué pa le logiciel, comme sur la version standard du Routeur Telindus 1421 SHDSL.

MU-9.6 Configuration RADIUS

Cette section présente le Romote Authentication Dial-In User Service (RADIUS) et fournit une description rapide des attributs que vous pouvez utiliser pour configurer RADIUS.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.6.1 - Introduction RADIUS page 292
- MU-9.6.2 - Configuration de RADIUS page 293
- MU-9.6.3 - Types d'attributs RADIUS supportés page 294
- MU-9.6.4 - Réglages IP de client (appelant) page 296
- MU-9.6.5 - Réglage IP NAS (appelé) page 296

MU-9.6.1 Introduction RADIUS

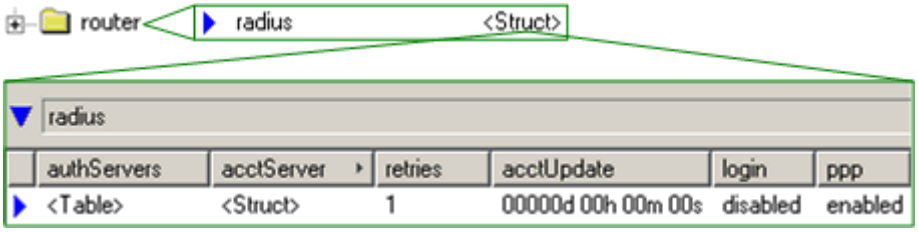
Qu'est-ce que le RADIUS?

Remote Authentication Dial-In User Service (RADIUS) est un protocole client/serveur et logiciel qui permet au Network Access Servers (NAS) de communiquer avec un serveur central pour authentifier les utilisateurs de numérotation et leur autoriser l'accès au système ou service demandé. RADIUS permet à une société de conserver les profils utilisateurs dans une base de données centrale que peuvent partager tous les serveurs distants. Il assure une meilleure sécurité, permettant à une société de configurer une politique pouvant être appliquée à un point de réseau administré de manière indépendante. Disposer d'un service central signifie également qu'il est plus facile de suivre l'utilisation en vue de la facturation et de l'élaboration de statistiques concernant le réseau.

MU-9.6.2 Configuration de RADIUS

Reportez-vous à MU-9.6.1 - Introduction RADIUS page 292 pour la présentation.

Pour configurer RADIUS, procédez de la façon suivante:

Etape	Action
1	Activez PAP ou CHAP sur le Routeur Telindus 1421 SHDSL.
2	Dans l'arborescence Routeur Telindus 1421 SHDSL, allez à l'objet router et sélectionnez l'attribut radius. 
3	Configurez les éléments de la structure radius. • authServers. Utilisez cet élément pour sélectionner un serveur d'authentification. Vous pouvez créer une liste de plusieurs serveurs d'authentification. • acctServer. Utilisez cet élément pour sélectionner un serveur comptable. Vous ne pouvez sélectionner qu'un seul serveur comptable. • retries. Utilisez cet élément pour spécifier le nombre de nouvelles tentatives avant de sélectionner le serveur d'authentification suivant dans la table authServers . • acctUpdate. Utilisez cet élément pour spécifier l'heure à laquelle une mise à jour des données comptables doit être envoyée au serveur. Réglez cet élément sur 0 (valeur par défaut) si aucune mise à jour n'est nécessaire. • login. Utilisez cet élément pour définir l'authentification d'accès au Routeur Telindus 1421 SHDSL en utilisant Telnet, FTP, TFTP ou TMA. Aucune donnée comptable n'est envoyée au serveur. • ppp. Utilisez cet élément pour définir l'authentification d'une connexion PPP utilisant PAP ou CHAP. Reportez-vous à telindus1421Router/router/radius page 94 pour de plus amples informations.

Notez que la configuration locale du nom d'utilisateur et du mot de passe est ignorée si une table de serveurs RADIUS existe. De plus, l'adresse IP distante et le masque distant sont ignorés si un serveur RADIUS impose ces attributs.

MU-9.6.3 Types d'attributs RADIUS supportés

Cette section indique quels types d'attributs RADIUS sont supportés par le Routeur Telindus 1421 SHDSL.

types d'attributs d'authentification RADIUS

(1) Nom d'utilisateur	Envoyé.
(2) Mot de passe d'utilisateur	Envoyé en cas d'authentification PAP, TELNET, FTP et TMA.
(3) Mot de passe CHAP	Envoyé en cas d'authentification CHAP.
(4) Adresse IP NAS	Envoyée (il s'agit de l'adresse IP de l'interface qui a reçu l'appel entrant).
(5) ID port NAS	Envoyée (il s'agit de l'indice de l'interface qui a reçu l'appel entrant).
(7) Protocole à trame	Envoyé.
(8) Adresse IP tramée	Supportée La configuration locale est subordonnée lors de la réception. • 255.255.255.255: le client peut choisir une adresse. Doit être rejeté si nulle. • 255.255.255.254: l'adresse IP distante qui est configurée sur le NAS est envoyée au client distant. • n'importe quelle adresse valable: cette adresse est prise comme adresse IP distante Voyez également MU-9.6.4 - Réglages IP de client (appelant) page 296 et MU-9.6.5 - Réglage IP NAS (appelé) page 296 pour la réaction NAS et du client distant lors de la réception / de l'apprentissage d'adresses IP et de masques.
(9) Masque IP tramé	Supportée Voyez également MU-9.6.4 - Réglages IP de client (appelant) page 296 et MU-9.6.5 - Réglage IP NAS (appelé) page 296 pour la réaction NAS et du client distant lors de la réception / de l'apprentissage d'adresses IP et de masques.
(22) Acheminement à trame	Supporté (1 métrique).
(25) Classe	Utilisé pour envoyer “accessRights” lors de l'utilisation de TELNET et TMA. Envoyée sous forme de valeur hexadécimale.
(27) Expiration de session	Supportée
(32) Identificateur NAS	Envoyé (= sysName)
(33) Etat proxy	
(60) Challenge CHAP	Envoyé.
(62) Limite de port	Supportée en cas de liaisons multiples.
(80) Authentificateur de message	Authentification HMAC MD5 de demande d'accès. Non nécessaire mais envoyée pour des raisons de sécurité.

types d'attributs comptables RADIUS

(40) Type d'état	Supporté (valeurs (1) Start, (2) Stop et (3) Update).
(41) Temporisation	Supportée
(42) Octets d'entrée	Supportée
(43) Octets de sortie	Supportée
(44) ID de session	Supportée
(45) Authentique	Supporté (toujours valeur (1) RADIUS).
(46) Heure de session	Supportée
(47) Paquets d'entrée	Supportée
(48) Paquets de sortie	Supportée
(49) Motif de terminaison	Supporté (valeurs (2) Perte de porteuse, (5) Expiration de session et (6) Admin Reset).
(50) ID multi-sessions	Supportée en cas de liaisons multiples.
(51) Comptage de liaison	Supportée en cas de liaisons multiples.

MU-9.6.4 Réglages IP de client (appelant)

La table qui suit illustre certains cas d'adresses IP que le client peut apprendre sur sa liaison PPP en cas de RADIUS:

Cas	Description
1	Adresse IP et masque déjà configurés sur le client. ⇒Utilisation d'adresse IP et de masque configurés
2	Aucune adresse IP ni masque ne sont configurés sur le client, ils sont appris depuis NAS. ⇒Cas normal: ajoutez 3 acheminements (hôte, réseau et diffusion). Cependant, si le masque appris est 255.255.255.252, aucun acheminement de diffusion n'est ajouté. Si le masque appris est 255.255.255.255, seul un acheminement hôte est ajouté. ⇒Si le gatewayPreference n'est pas 0, une passerelle par défaut est ajoutée via l'interface PPP avec la préférence configurée. ⇒Si la liaison PPP est défaillante, supprimez tous les acheminements.
3	Aucune adresse IP n'est configurée sur le client. L'adresse IP est apprise depuis NAS, pas le masque. ⇒L'adresse IP configurée est utilisée. ⇒Réglez le masque sur 255.255.255.255.
4	Le client est configuré en mode non numéroté (une adresse IP et un masque sont pris d'une autre interface pour laquelle l'adresse IP et le masque sont configurés). ⇒L'adresse IP et le masque de l'interface de référence sont utilisés.

MU-9.6.5 Réglage IP NAS (appelé)

La table qui suit illustre certains cas d'adresses IP que le NAS définit sur sa liaison PPP en cas de RADIUS:

Cas	Description
1	Une adresse IP et un masque sont configurés en mode ou le mode non numéroté est configuré. Le client distant demande une adresse IP et un masque. ⇒Si l'adresse IP distante ne correspond pas au réseau défini par l'adresse IP propre et le masque, rejet de l'option VSO 0.0.0.0 depuis l'autre extrémité. (P. ex. IP distante = 10.0.0.1 et IP propre = 192.168.0.1 / 255.255.255.0.) ⇒Si (adresse IP distante et masque) = (adresse IP locale et masque), un acheminement d'hôte est ajouté pour l'adresse IP distante, aux fins de s'assurer que l'adresse distante peut être atteinte (via ARP proxy lorsque le NAS est en mode non numéroté).

MU-9.7 Configuration QoS

Cette section présente la qualité de service (QoS) et, à l'aide de schémas, essaie de montrer quels attributs vous pouvez utiliser pour configurer QoS.

Le tableau suivant donne un aperçu de ce chapitre:

- MU-9.7.1 - Présentation QoS page 298
- MU-9.7.2 - IP QoS page 299
- MU-9.7.3 - VLAN QoS page 300
- MU-9.7.4 - QoS sur une interface Ethernet page 300
- MU-9.7.5 - QoS sur une interface PPP sans fragmentation page 301
- MU-9.7.6 - QoS sur une interface PPP avec fragmentation page 301
- MU-9.7.7 - QoS sur une interface PPPmultiliaisons avec fragmentation page 302
- MU-9.7.8 - QoS sur une interface à Frame Relay sans fragmentation page 303
- MU-9.7.9 - QoS sur une interface à Frame Relay avec fragmentation page 303
- MU-9.7.10 - QoS sur une interface à Frame Relay multiliaisons sans fragmentation page 304
- MU-9.7.11 - QoS sur une interface à Frame Relay multiliaisons avec fragmentation page 305
- MU-9.7.12 - Options de fragmentation de Frame Relay page 305
- MU-9.7.13 - QoS sur une interface ATM page 306
- MU-9.7.14 - QoS sur une interface ATM IMA page 306

MU-9.7.1 Présentation QoS

Qu'est-ce que QoS?

La qualité de service (QoS) est la capacité d'un réseau à fournir un meilleur service pour un trafic réseau donné utilisant diverses technologies (p. ex. Frame Relay, ATM, Ethernet et réseaux IP utilisant une ou plusieurs de ces technologies sous-jacentes). L'objectif premier de la QoS est d'assurer la priorité, y compris une largeur de bande dédiée, un contrôle des oscillations et de la latence, et des pertes moindres. Il est également important de s'assurer que la mise en priorité d'un ou de plusieurs flux n'entraîne pas la défaillance des autres flux.

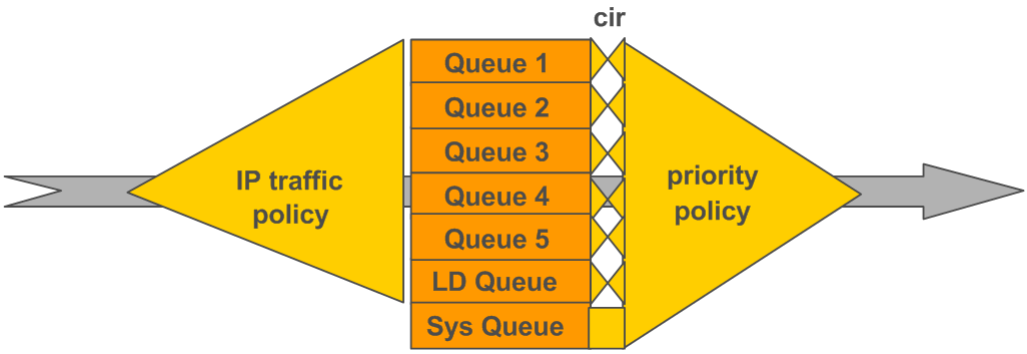
QoS n'est pas un attribut dont vous pouvez régler la qualité sur “basse”, “moyenne” ou “élevée”. QoS est un *ensemble* d'attributs de configuration situés à différents niveaux (p. ex. file d'attente, fragmentation PPP, contrôle de largeur de bande, etc.).

La table qui suit donne un aperçu des fonctions qui peuvent être utilisées pour la QoS:

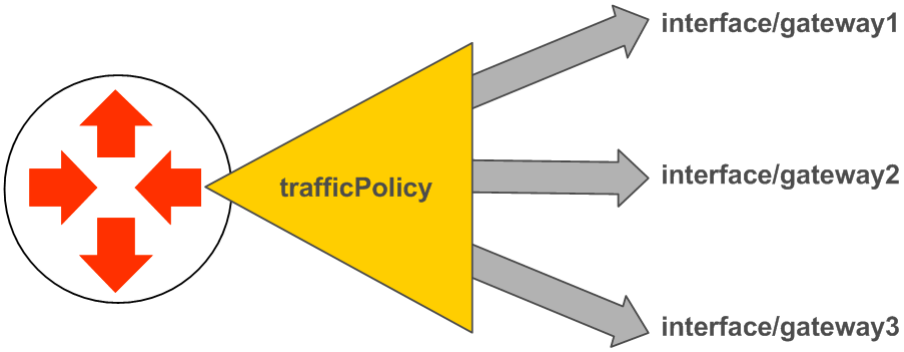
Protocole	**Fonction**
Tous	7 files: 5 files configurables par l'utilisateur, une file à faible temporisation et une file système.
Tous	Politiques de priorité: FIFO, round robin, priorité absolue, WFQ, WFQ à faible temporisation.
Tous	Contrôle de largeur de bande par file avec valeurs CIR .
IP	Classification de trafic IP sur la base des listes d'accès (trafficShaping), tosDiffServ & tosMapped.
VLAN	Classification trafic VLAN basé sur 802.1P bits.
PPP	Fragmentation PPP.
PPP	Multiclasses PPP.
PPP	Meilleur équilibre de charge pour MLPPP.
Frame Relay	Fragmentation de Frame Relay.
Frame Relay	CIR / EIR sur trafic sortant.
Frame Relay	CIR / EIR sur trafic entrant.
ATM	Classe de trafic UBR.

MU-9.7.2 IP QoS

- 7 files par interface.
  - File 1 à 5.
  - File à faible temporisation.
  - File système pour, p. ex. les protocoles de commande (PPP LCP, Frame Relay LMI, ATM OAM, …).
  - CIR configurable par file (à l'exception de la file système).
- Politique de trafic: affecte le trafic IP à une file.
  - Modélisation de trafic: classification sur adresses IP, protocole IP, numéros de ports UDP/TCP et bits TOS.
  - diffServ: affectation fixe aux files et 3 niveaux de rejet basés sur 2 bits TOS.
  - affectation TOS: affectation configurable sur bits TOS uniquement.
- Politique de priorité: définit la politique de vidage des files.
  - FIFO, round robin, priorité absolue, WFQ, WFQ à faible temporisation.
  - Commande de largeur de bande par file (CIR).
  - La file système a toujours la priorité absolue.

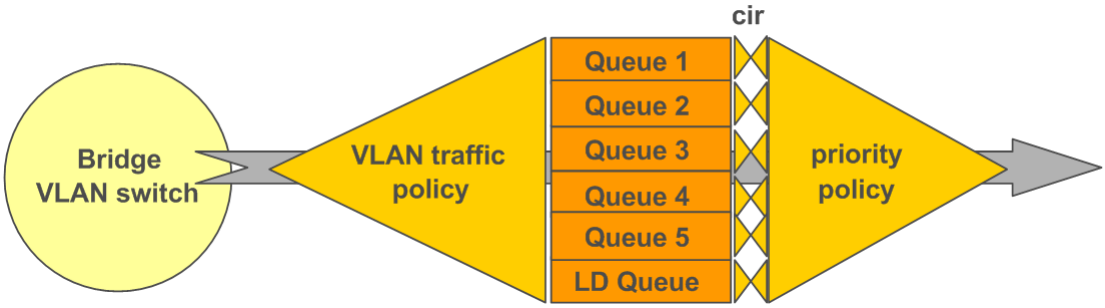


- Acheminement en fonction de la politique: l'acheminement est basé sur les protocoles de couches supérieures.
  - Adresses IP, protocole IP, numéros de ports UDP/TCP et bits TOS.



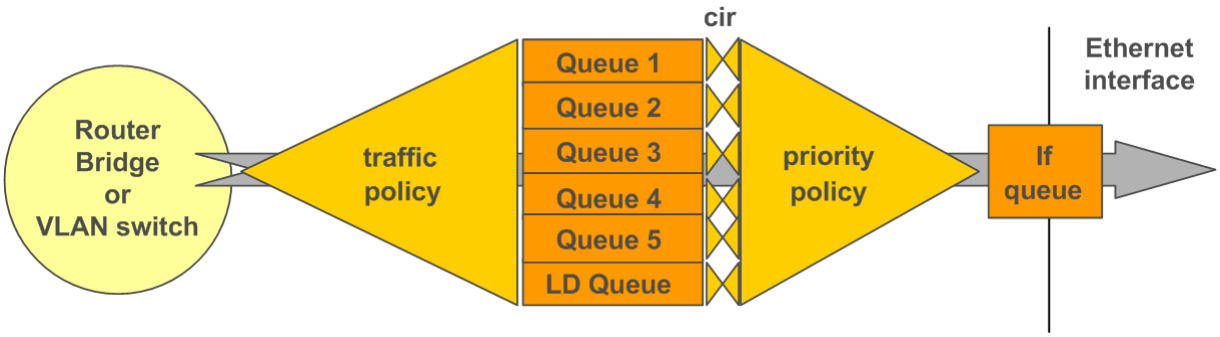
MU-9.7.3 VLAN QoS

- Uniquement en cas de pontage ou de mode de commutation VLAN.
- Applicable uniquement sur paquets VLAN (utilisant les bits P).
- Politique de trafic basée sur la valeur des bits P.
- Affectation IP TOS à VLAN COS en cours d'identification.



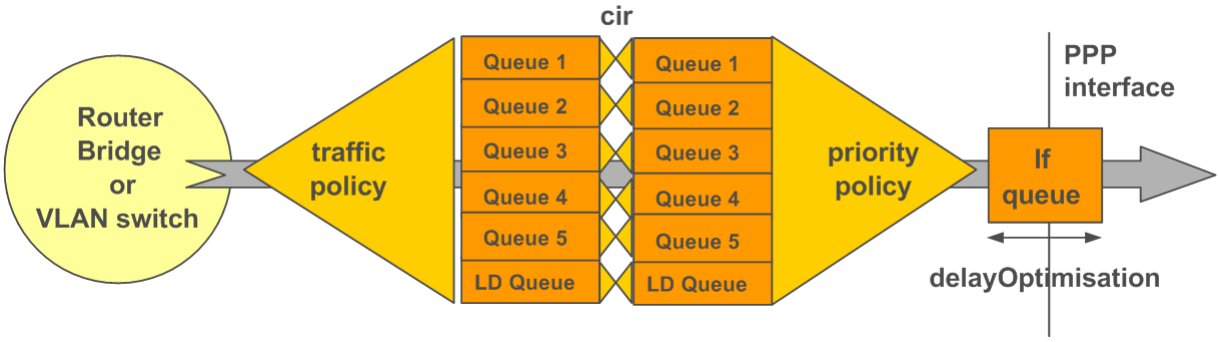
MU-9.7.4 QoS sur une interface Ethernet

- Les politiques de trafic et de priorité sont configurées au niveau de l'interface physique.
- CIR est configurable par file.



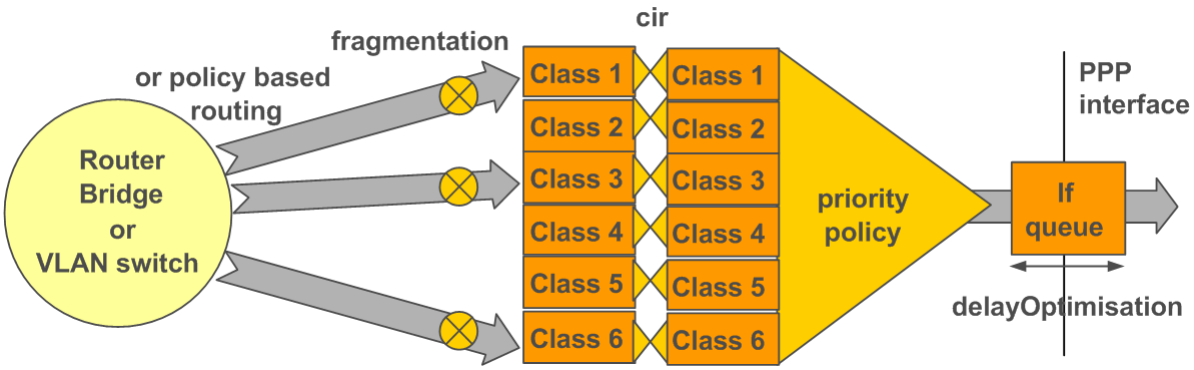
MU-9.7.5 QoS sur une interface PPP sans fragmentation

- Les politiques de trafic et de priorité sont configurées au niveau de l'interface physique.
- CIR est configurable par file.
- Lors du réglage de l'attribut delayOptimisation sur lowSpeedLinks, la longueur de la file d'interface est alors réduite. Cela s'avère particulièrement intéressant pour les liaisons à faible vitesse.



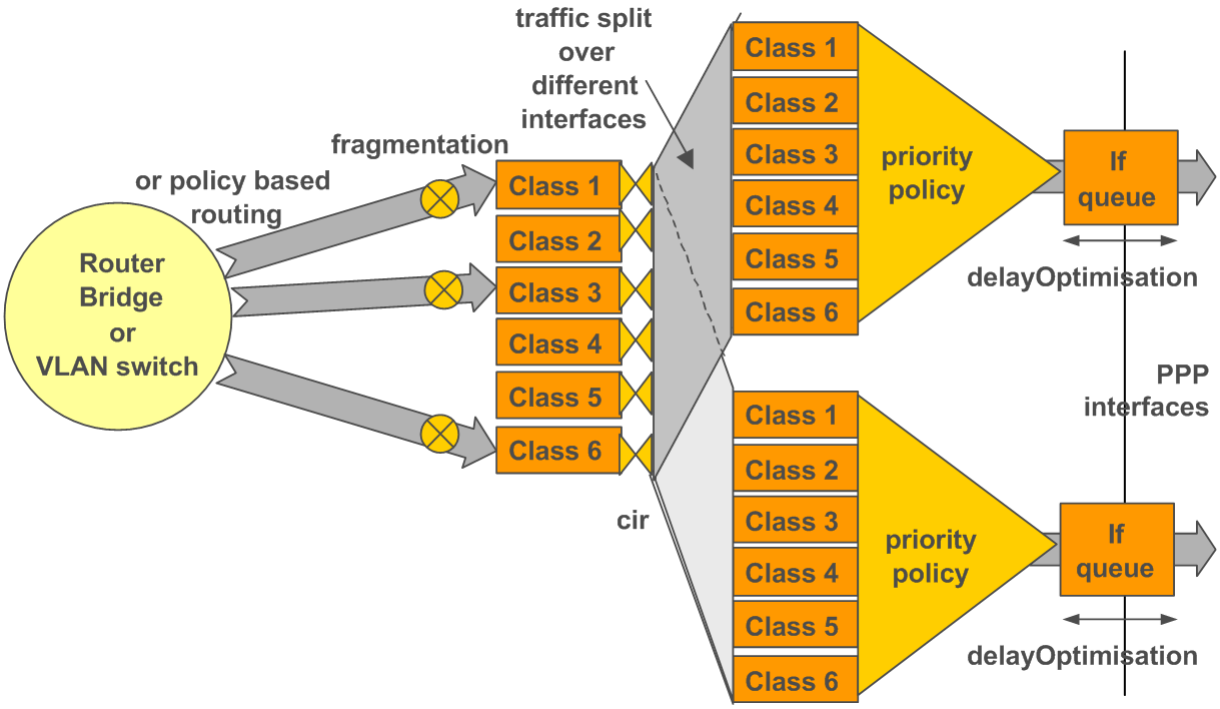
MU-9.7.6 QoS sur une interface PPP avec fragmentation

- La fragmentation sur PPP est le plus souvent utilisée pour QoS (en particulier si la vitesse de la liaison est inférieure à 2 Mbps).
- La fragmentation peut être activée ou désactivée pour chaque interface (et non par classe).
- Utilisez PPP multiclasses pour QoS.
  - Configurez un faisceau PPP pour pouvoir utiliser la multiclasse.
  - Chaque classe est semblable à une interface distincte.
  - Chaque classe utilise une file de priorité (configurable par classe). Il n'est pas nécessaire d'appliquer une politique de trafic (utilisez la file par défaut).
  - Appliquez une politique de priorité à l'interface physique.



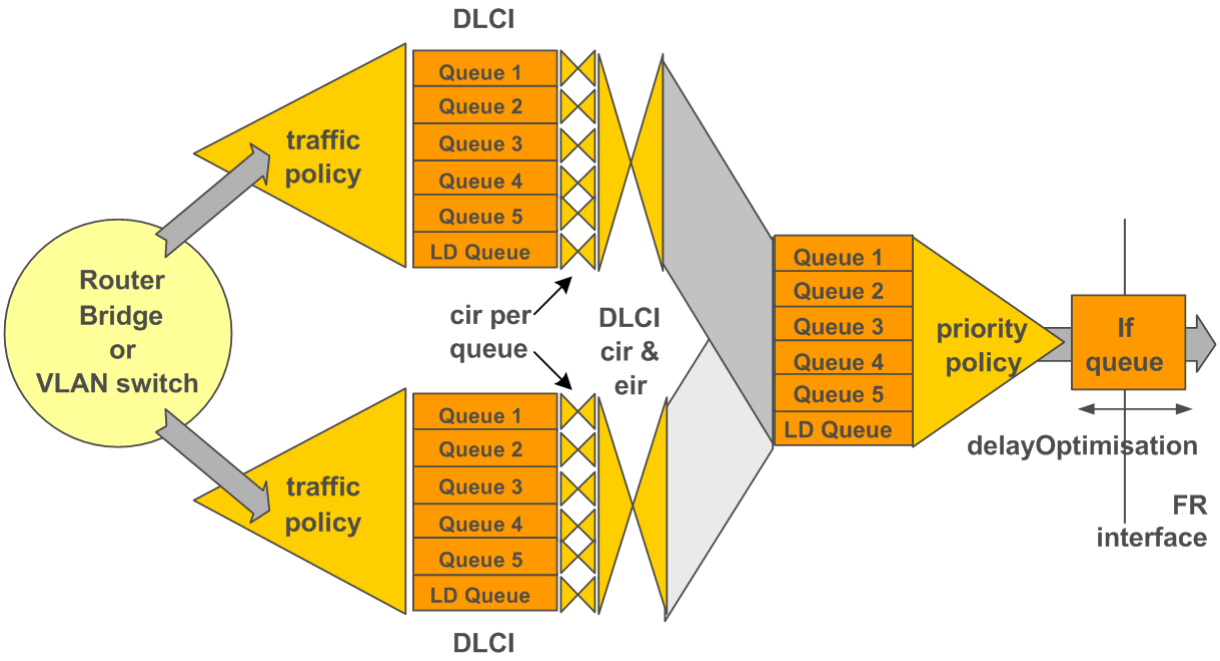
MU-9.7.7 QoS sur une interface PPPmultiliaisons avec fragmentation

Similaire à MU-9.7.6 - QoS sur une interface PPP avec fragmentation page 301, si ce n'est que vous utilisez maintenant plusieurs interfaces physiques.



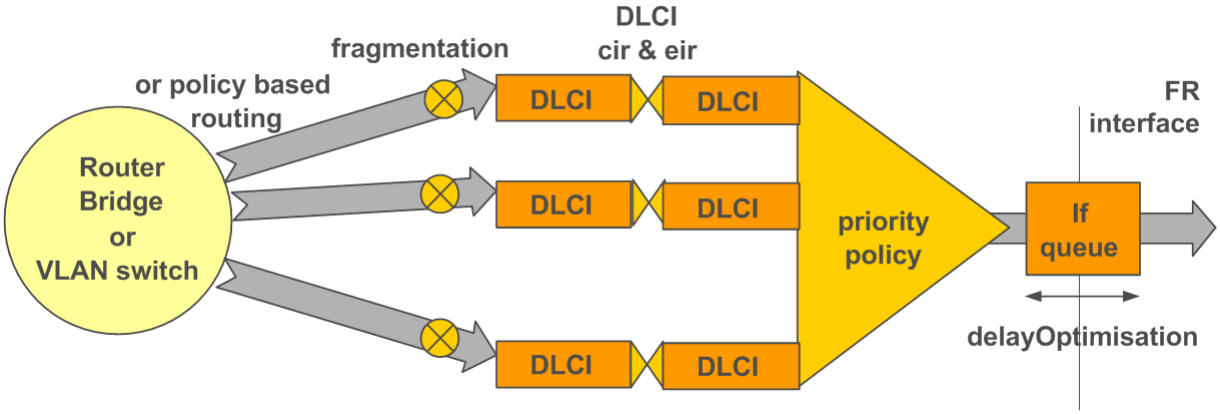
MU-9.7.8 QoS sur une interface à Frame Relay sans fragmentation

- La politique de trafic est configurée au niveau DLCI.
- La politique de priorité est configurée au niveau de l'interface physique.
- CIR est configurable par file et par DLCI.



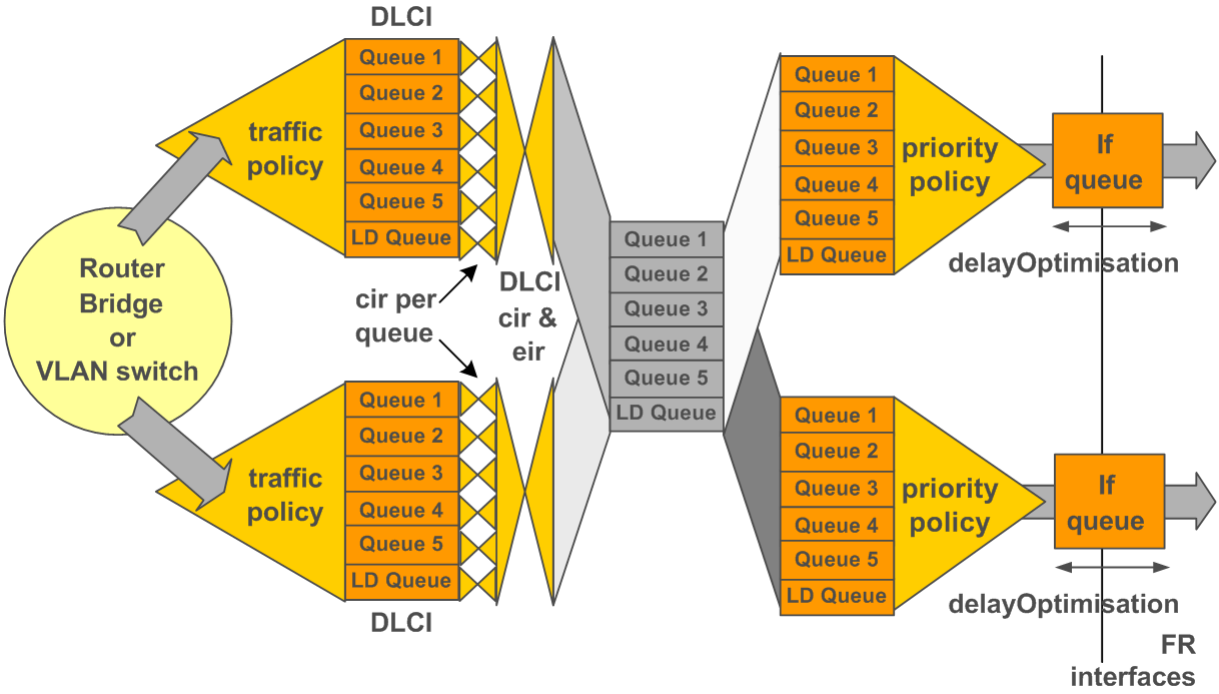
MU-9.7.9 QoS sur une interface à Frame Relay avec fragmentation

- Utilisez des DLCI multiples par destination pour différentes classes de trafic.
- Chaque DLCI utilise une file de priorité (configurable par DLCI). Il n'est pas nécessaire d'appliquer une politique de trafic (utilisez la file par défaut).
- La politique de priorité est configurée au niveau de l'interface physique. .



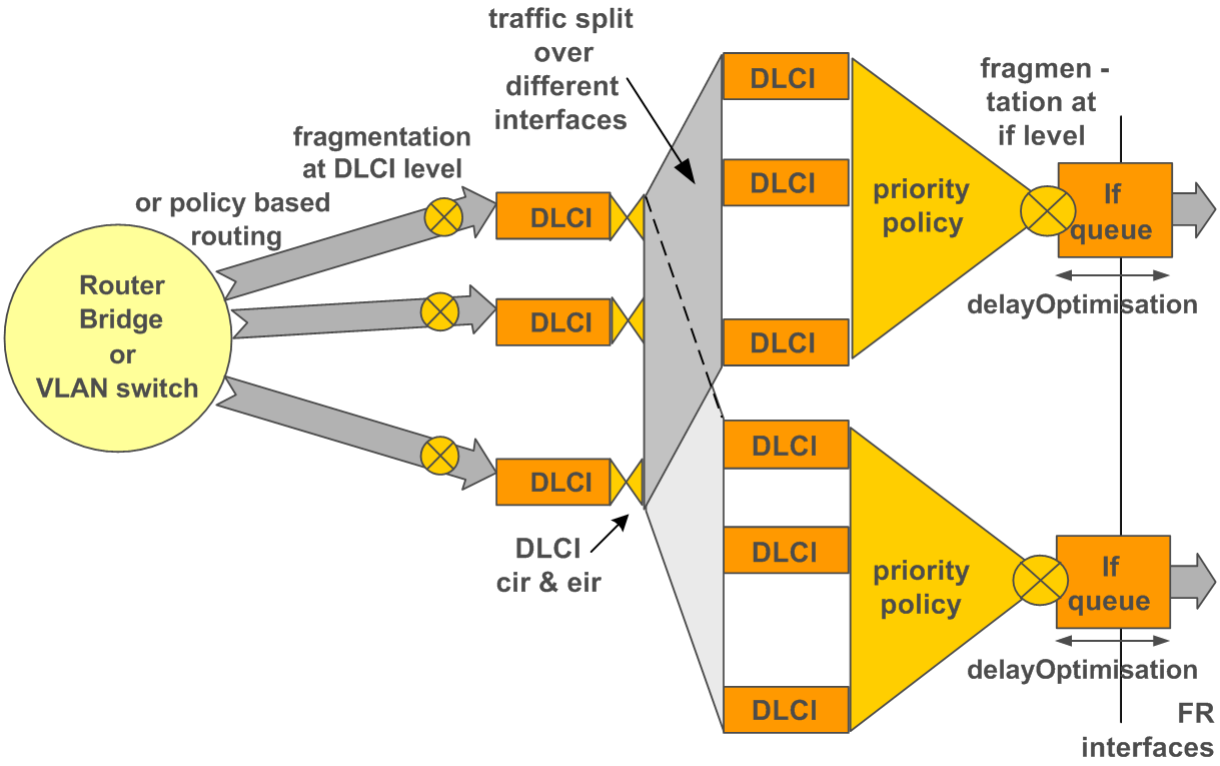
MU-9.7.10 QoS sur une interface à Frame Relay multiliaisons sans fragmentation

- Configurez un faisceau de Frame Relay.
- La politique de trafic est configurée au niveau DLCI.
- La politique de priorité est configurée au niveau de l'interface physique.
- CIR est configurable par file et par DLCI.



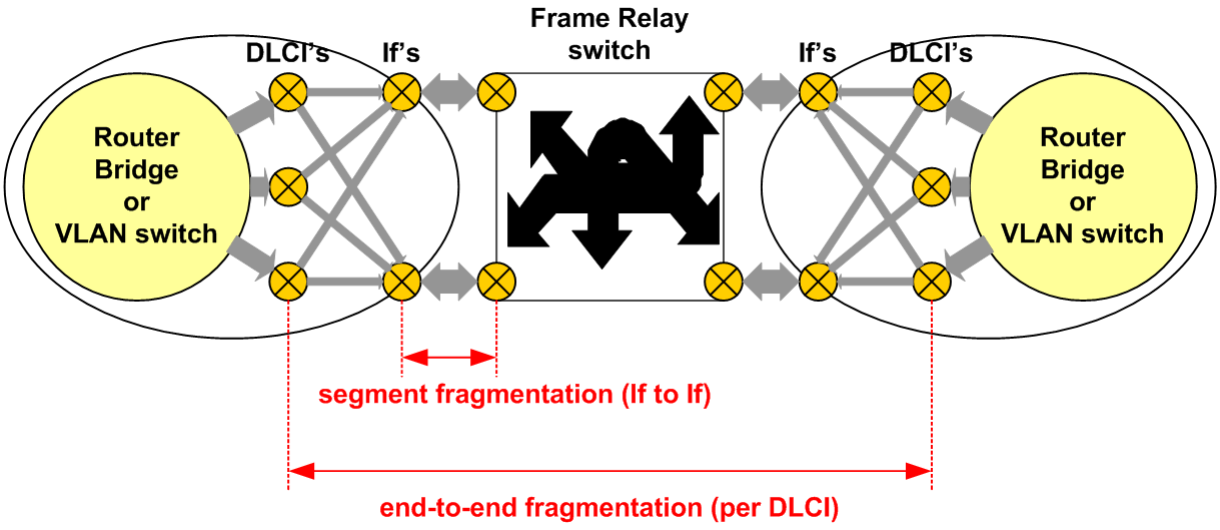
MU-9.7.11 QoS sur une interface à Frame Relay multiliaisons avec fragmentation

- Configurez un faisceau de Frame Relay.
- Appliquez les mêmes principes QoS sur l'interface du faisceau que sur l'interface physique.
- Notez que les routeurs Cisco ne supportent pas la fragmentation sur une interface à Frame Relay multiliaisons.



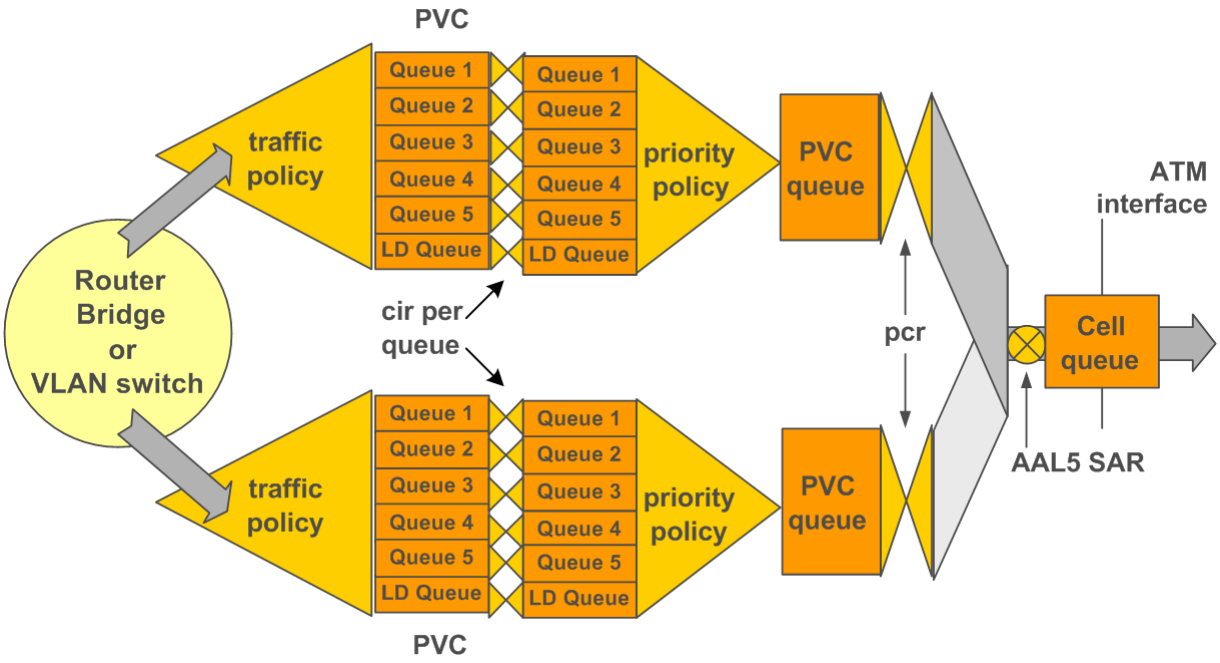
MU-9.7.12 Options de fragmentation de Frame Relay

- Fragmentation de bout en bout = fragmentation au niveau DLCI.
- Fragmentation de segment = fragmentation au niveau de l'interface (jusqu'à un commutateur).

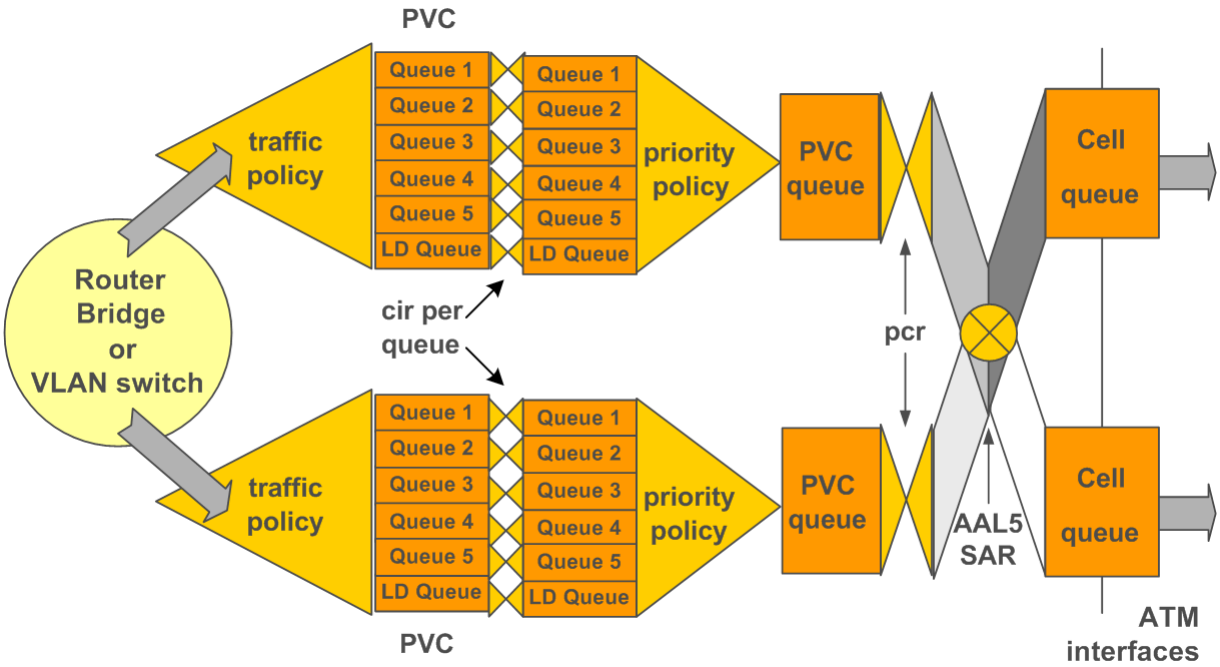


MU-9.7.13 QoS sur une interface ATM

- Chaque PVC se comporte comme une interface physique.
- Les politiques de trafic et de priorité sont configurées au niveau PVC.
- CIR est configurable par file.
- PCR est configurable par PVC.
- AAL5 SAR (= fragmentation) se produit à la fin.



MU-9.7.14 QoS sur une interface ATM IMA



MU-10 Exemples de configuration

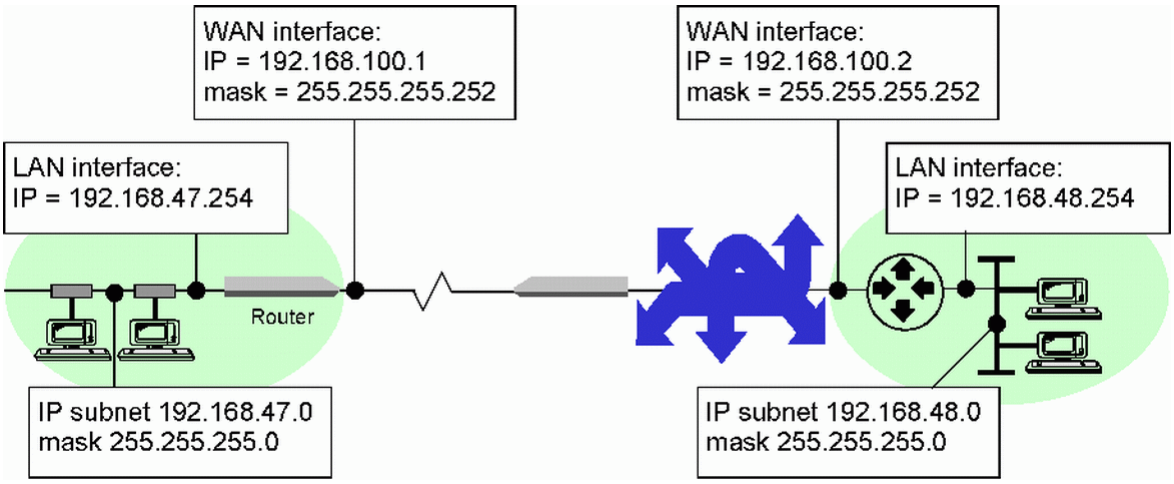
Ce chapitre donne quelques exemples de configuration du Routeur Telindus 1421 SHDSL. Le tableau suivant donne un aperçu de ce chapitre:

- MU-10.1 - Extension LAN par un réseau PDH/SDH page 309
- MU-10.2 - Extension LAN par un réseau à Frame Relay page 311
- MU-10.3 - Extension LAN par un réseau ATM page 313
- MU-10.4 - Connexion d'un LAN à l'internet en utilisant NAT et PAT page 315
- MU-10.5 - Utilisation de PAT avec un minimum d'adresses IP officielles page 317
- MU-10.6 - Combinaison de pontage et d'acheminement dans un réseau page 319
- MU-10.7 - Connexion de deux réseaux par un tunnel page 321
- MU-10.8 - Connexion de commutateurs à activation VLAN par un WAN page 324
- MU-10.9 - Multiplexage VLAN page 326
- MU-10.10 - Utilisation des listes d'accès étendu page 329

MU-10.1 Extension LAN par un réseau PDH/SDH

Dans cet exemple, un bureau distant est connecté à un bureau central par un réseau PDH ou SDH.

Une liaison modem connecte le bureau distant au réseau PDH ou SDH. Au bureau local, un Routeur Telindus 1421 SHDSL est installé. Le routeur central est un routeur tiers. L'encapsulation WAN est PPP avec une surveillance de liaison active.



La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

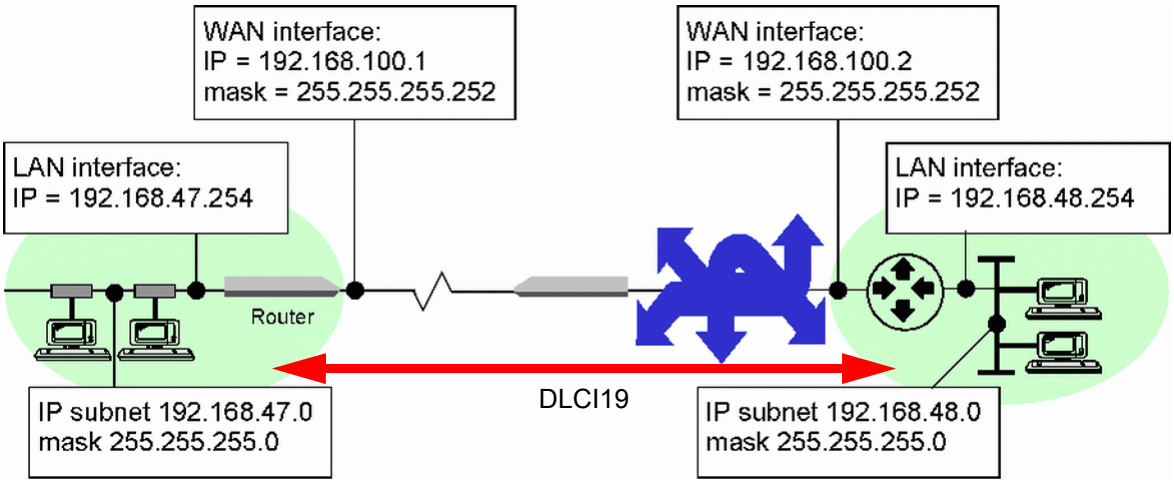
```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = ppp
    }
    SELECT ppp
    {
      LIST
      {
        ip =
        {
          adresse = 192.168.100.1
          netMask = 255.255.255.252
        }
        mode = routing
        linkMonitoring =
        {
          operation = enabled
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      routingTable =
      {
        [a] =
```

```
        {
          réseau = 192.168.48.0
          passerelle = 192.168.100.2
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.2 Extension LAN par un réseau à Frame Relay

Dans cet exemple, un bureau distant est connecté à un bureau central par un réseau à Frame Relay.

Une liaison modem connecte le bureau distant au réseau à Frame Relay. Au bureau local, un Routeur Telindus 1421 SHDSL est installé. Le routeur central est un routeur tiers.Le réseau à Frame Relay utilise LMI conformément à la norme ANSI. Aucun Inverse ARP n'est supporté par le réseau.



La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

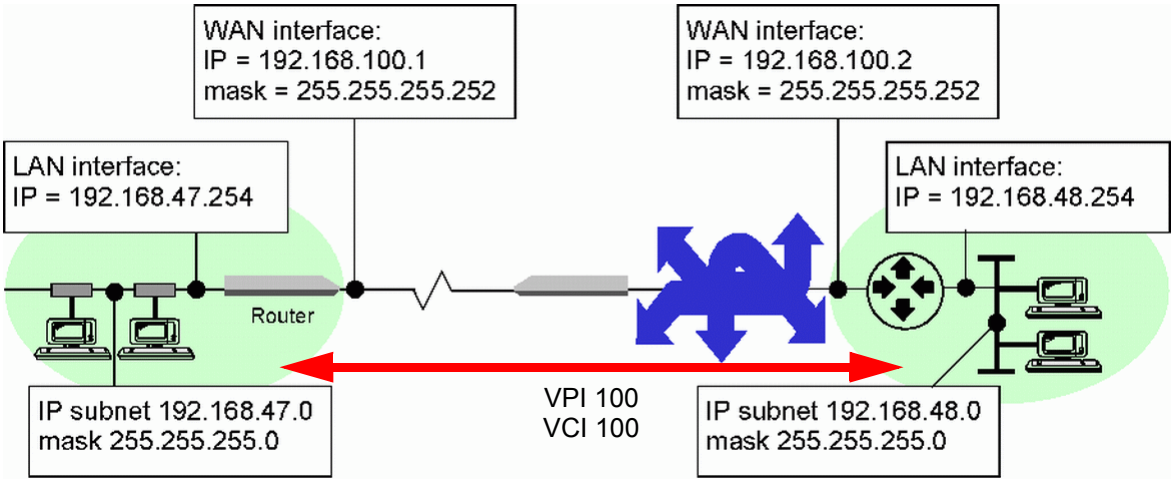
```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = frameRelay
    }
    SELECT frameRelay
    {
      LIST
      {
        dlciTable =
        {
          [a] =
          {
            nom = dlci1
            ip =
            {
              adresse = 192.168.100.1
              netMask = 255.255.255.252
              distant = 192.168.100.2
            }
            frameRelay =
            {
              dlci = 19
            }
          }
        }
        lmi =
        {
          type = ansiT1-617-d
```

```
        }
      }
    }
  }
  SELECT router
  {
    LIST
    {
      routingTable =
      {
        [a] =
        {
          réseau = 192.168.48.0
          passerelle = 192.168.100.2
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.3 Extension LAN par un réseau ATM

Dans cet exemple, un bureau distant est connecté à un bureau central par un réseau ATM.

Une liaison modem connecte le bureau distant au réseau ATM. Au bureau local, un Routeur Telindus 1421 SHDSL est installé. Le routeur central est un routeur tiers.



La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

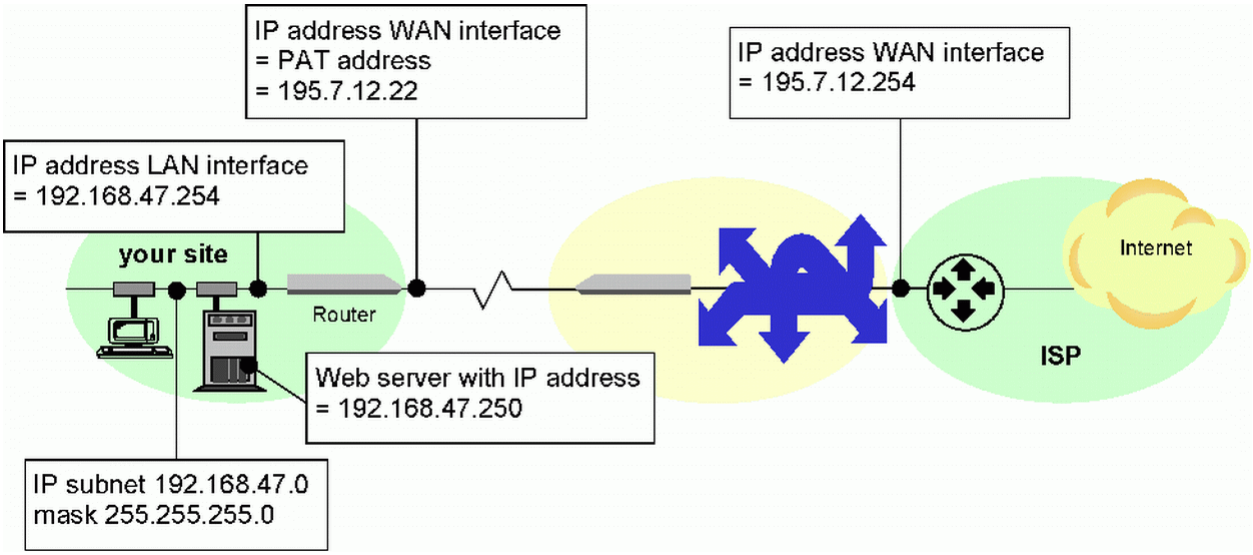
```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = atm
    }
    SELECT atm
    {
      LIST
      {
        pvcTable =
        {
          [a] =
          {
            nom = pvc1
            ip =
            {
              adresse = 192.168.100.1
              netMask = 255.255.255.252
              distant = 192.168.100.2
            }
            atm =
            {
              vpi = 100
              vci = 100
            }
          }
        }
      }
    }
  }
  SELECT router
```

```
  {
    LIST
    {
      routingTable =
      {
        [a] =
        {
          réseau = 192.168.48.0
          passerelle = 192.168.100.2
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.4 Connexion d'un LAN à l'internet en utilisant NAT et PAT

Il s'agit d'un exemple de réseau local qui utilise uniquement des adresses privées.

A PPP connecte votre site au fournisseur de service internet. Sur votre site est installé un Routeur Telindus 1421 SHDSL. Vous n'avez reçu que 2 adresses IP officielles du fournisseur, une pour tout le trafic sortant utilisant PAT (195.7.12.22) et une pour accéder au serveur web local utilisant NAT (195.7.12.21) avec une adresse privée dédiée.



La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

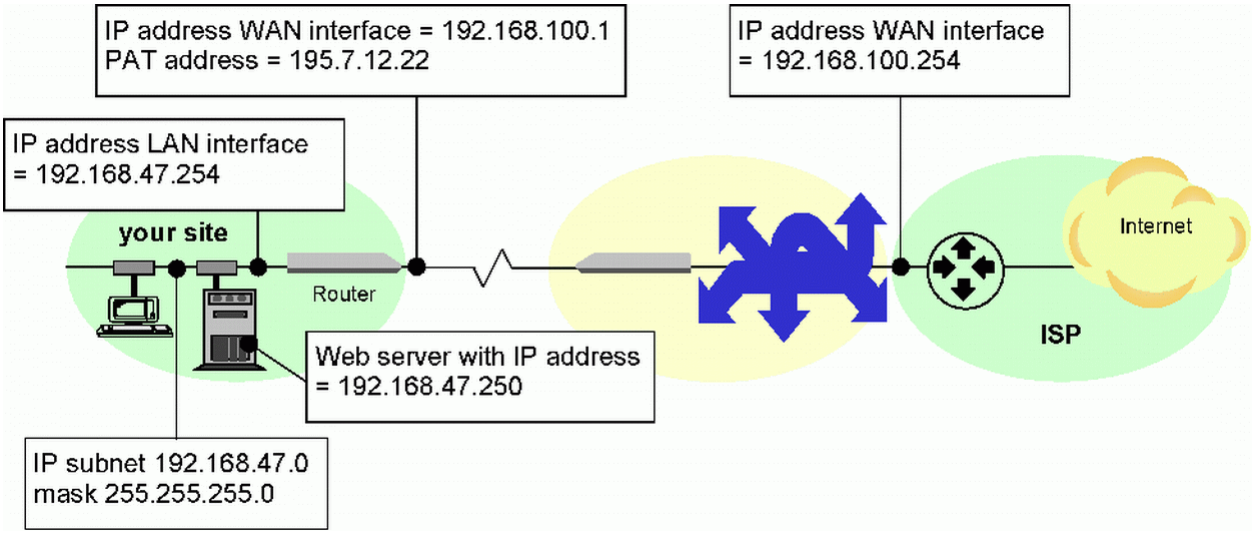
```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = ppp
    }
    SELECT ppp
    {
      LIST
      {
        ip =
        {
          adresse = 195.7.12.22
          nat = default
        }
        mode = routing
      }
    }
  }
  SELECT router
  {
    LIST
    {
      defaultRoute =
      {
        passerelle = 195.7.12.254
```

```
      }
    }
    SELECT defaultNat
    {
      LIST
      {
        patAddress = 195.7.12.22
        adresses =
        {
          [a] =
          {
            officialAddress = 195.7.12.21
            privateAddress = 192.168.47.250
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.5 Utilisation de PAT avec un minimum d'adresses IP officielles

Il s'agit d'un autre exemple de réseau local qui utilise uniquement des adresses privées.

A PPP connecte votre site au fournisseur de service internet. Sur votre site est installé un Routeur Telindus 1421 SHDSL. Vous n'avez reçu qu'une seule adresse IP officielle du fournisseur d'accès. Pour réduire le nombre d'adresses IP officielles, le fournisseur d'accès utilise également des adresses IP privées sur la liaison. La table d'acheminement du routeur central a un chemin hôte vers son adresse PAT par client.



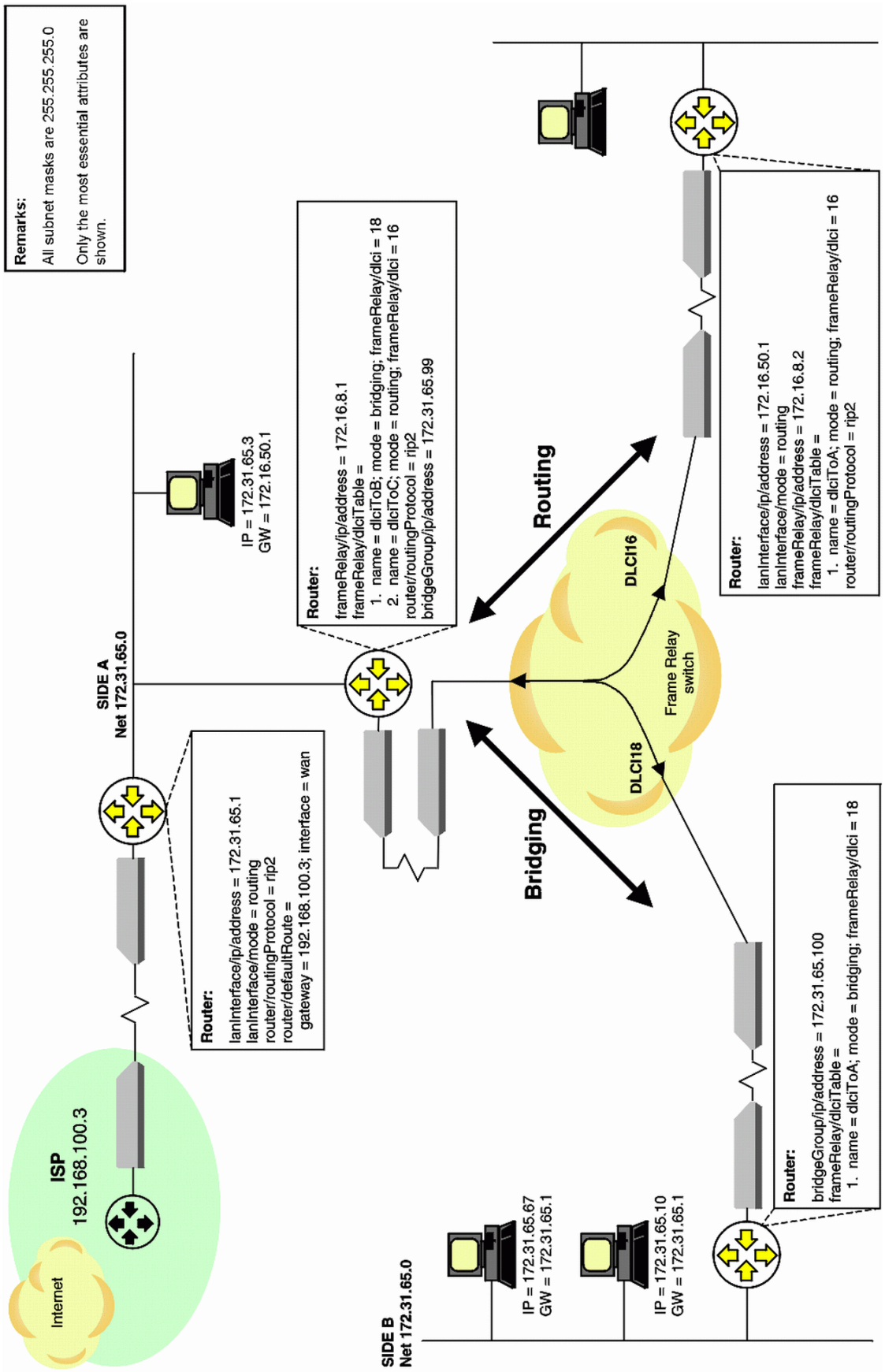
La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 192.168.47.254
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = ppp
    }
    SELECT ppp
    {
      LIST
      {
        ip =
        {
          adresse = 192.168.100.1
          nat = default
        }
        mode = routing
      }
    }
  }
  SELECT router
  {
    LIST
    {
```

```
      defaultRoute =
      {
        passerelle = 192.168.100.254
      }
    }
    SELECT defaultNat
    {
      LIST
      {
        patAddress = 195.7.12.22
        servicesAvailable =
        {
          [a] =
          {
            protocol = tcp
            startPort = 80
            serverAddress = 192.168.47.250
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.6 Combinaison de pontage et d'acheminement dans un réseau

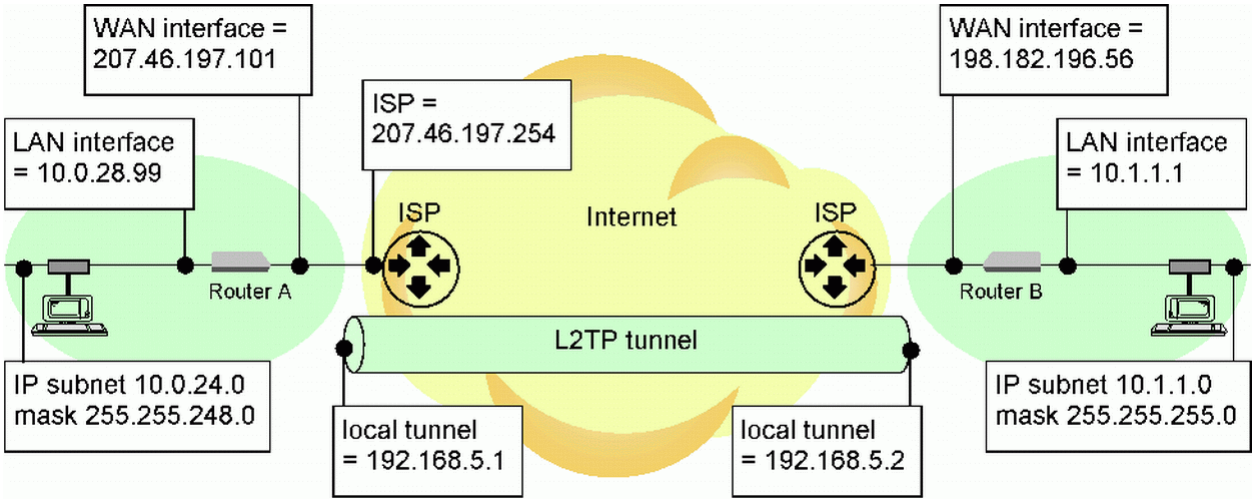
L'exemple qui suit montre une combinaison de pontage et d'acheminement dans un réseau:



MU-10.7 Connexion de deux réseaux par un tunnel

Il s'agit d'un exemple de deux réseaux connectés par deux Routeur Telindus 1421 SHDSLs par un tunnel sur l'internet.

Un chemin entre l'interface WAN des routeurs A et B doit exister au préalable. Le tunnel peut alors être configuré. Les routeurs A et B apprennent les chemins de leurs réseaux respectifs par RIP. Toutefois, ils ne doivent pas apprendre les adresses WAN et de tunnel IP. Par conséquent, un filtre est créé.



La configuration du routeur A en format CLI est alors la suivante:

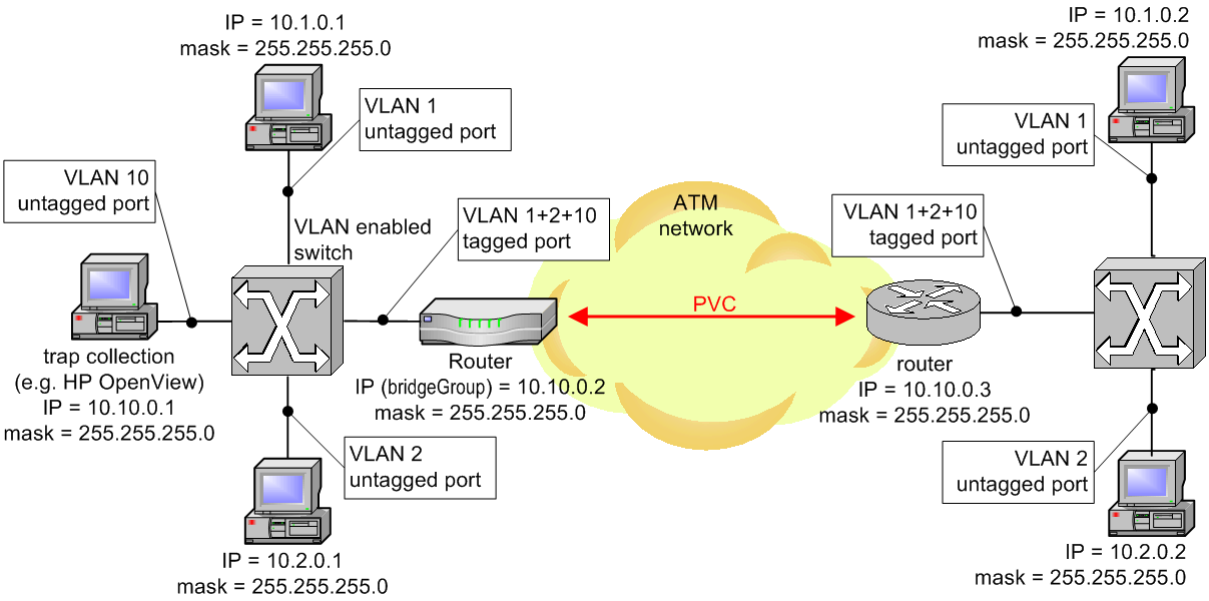
```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 10.0.28.99
        netMask = 255.255.255.0
        rip =
        {
          mode = disabled
        }
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = ppp
    }
    SELECT ppp
    {
      LIST
      {
        ip =
        {
          adresse = 207.46.197.101
          distant = 207.46.197.254
          rip =
          {
            mode = disabled
          }
        }
        mode = routing
      }
    }
  }
SELECT router
  {
    LIST
    {
      defaultRoute =
      {
        passerelle = 207.46.197.254
      }
      routingProtocol = rip2
    }
    SELECT tunnels
    {
      LIST
      {
        l2tpTunnels =
        {
          [a] =
          {
            nom = tunnel1
            ip =
            {
              adresse = 192.168.5.1
              distant = 192.168.5.2
              rip =
              {
                filtre = tunnelFilter
              }
            }
            l2tp =
            {
              localIpAddress = 207.46.197.101
              remoteIpAddress = 198.182.196.56
              type = outgoingLeasedLine
```

```
            }
          }
        }
      }
    }
    SELECT routingFilter[tunnelFilter]
    {
      LIST
      {
        filtre =
        {
          [a] =
          {
            réseau = 10.0.0.0
            masque = 255.0.0.0
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.8 Connexion de commutateurs à activation VLAN par un WAN

Il s'agit d'un exemple de 2 commutateurs à actionnement VLAN connectant des VLAN multiples par une liaison WAN. Dans cet exemple, VLAN 1 et 2 sont utilisés pour les données utilisateurs, alors que VLAN 10 est utilisé pour gérer le Routeur Telindus 1421 SHDSL et le routeur tiers distant.

Pour réaliser cette configuration, vous ne devez pas explicitement créer des VLAN sur l'interface LAN en utilisant la table vlan. Cela est dû au fait que l'interface LAN accepte à la fois des données VLAN non identifiées et VLAN identifiées. Les données VLAN non identifiées sont pontées et/ou acheminées (en fonction du réglage de l'attribut de configuration lanInterface/mode). Les données VLAN identifiées sont pontées (si l'attribut de configuration lanInterface/mode est réglé sur bridging ou bridgingAndRouting, sinon, elles sont rejetées).



La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      mode = bridging
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = atm
    }
    SELECT atm
    {
      LIST
      {
        pvcTable =
        {
          [a] =
          {
            nom = pvc1
            mode = bridging
            atm =
            {
              vpi = 100
```

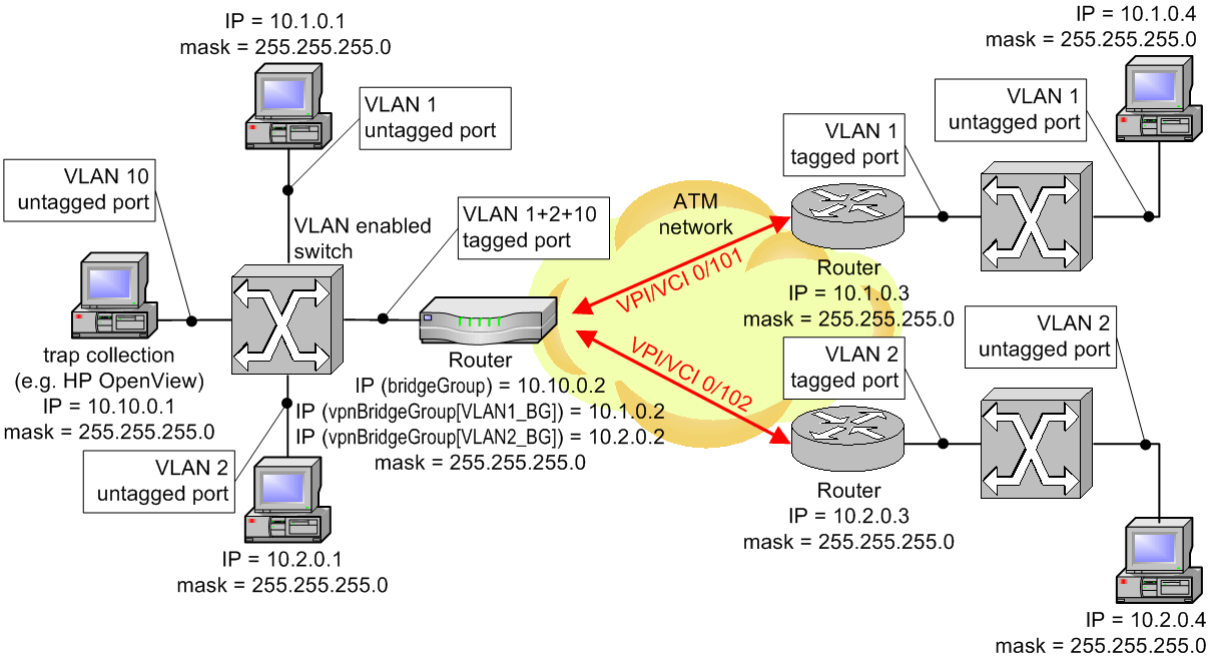
```
              vci = 100
            }
          }
        }
      }
    }
  }
  SELECT bridge
  {
    SELECT bridgeGroup
    {
      LIST
      {
        ip =
        {
          adresse = 10.1.0.2
        }
        vlan =
        {
          dotQTagging = enabled
          vid = 10
        }
      }
    }
  }
}
action "Activate Configuration"
```

MU-10.9 Multiplexage VLAN

Il s'agit d'un exemple de multiplexage VLAN. Dans cet exemple, deux réseaux distants sont “concentrés” dans le Routeur Telindus 1421 SHDSL. Pour distinguer les données d'un réseau des données de l'autre, 2 VLAN sont créés. Dans cet exemple, les VLAN 1 et 2 transportent les données provenant des deux réseaux distants, tandis que le VLAN 10 est utilisé pour gérer le Routeur Telindus 1421 SHDSL.

Les VLAN 1 et 2 sont configurés dans la table vlan. Les 2 ATM PVC connectés aux réseaux distants sont configurés dans pvcTable. Chaque paire VLAN - ATM PVC est affectée à un groupe de pontage différent.

Le VLAN 10 est configuré dans la table vlan. La session de gestion se termine au Routeur Telindus 1421 SHDSL, les identifications VLAN ne doivent pas être transmises, c'est-à-dire qu'elles peuvent être supprimées. De plus, VLAN 10 est affecté au groupe de pontage par défaut. Dans ce groupe de pontage, dotQTagging est activé.




```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      mode = bridging
      vlan =
      {
        [a] =
        {
          nom = "VLAN1_LAN"
          mode = bridging
          bridging =
          {
            bridgeGroup = "VLAN1_BG"
          }
          vlan =
          {
            vid = 1
            tagSignificance = "global"
          }
        }
        [a] =
        {
          nom = "VLAN2_LAN"
          mode = bridging
          bridging =
```

```
        {
          bridgeGroup = "VLAN2_BG"
        }
        vlan =
        {
          vid = 2
          tagSignificance = "global"
        }
      }
      [a] =
      {
        nom = "VLAN10_MGT"
        mode = bridging
        vlan =
        {
          vid = 10
          tagSignificance = "local"
        }
      }
    }
  }
}
SELECT wanInterface
{
  LIST
  {
    encapsulation = "atm"
  }
  SELECT atm
  {
    LIST
    {
      pvcTable =
      {
        [a] =
        {
          nom = "VLAN1_WAN"
          mode = "bridging"
          bridging =
          {
            bridgeGroup = "VLAN1_BG"
          }
          atm =
          {
            vpi = 0
            vci = 101
          }
        }
        [a] =
        {
          nom = "VLAN2_WAN"
          mode = "bridging"
          bridging =
          {
            bridgeGroup = "VLAN2_BG"
          }
          atm =
          {
            vpi = 0
            vci = 102
          }
        }
      }
    }
  }
}
SELECT bridge
{
  SELECT bridgeGroup
  {
    LIST
    {
      ip =
      {
        adresse = 10.10.0.2
      }
      vlan =
      {
```

```
          dotQTagging = "enabled"
          vid = 10
        }
      }
    }
    SELECT vpnBridgeGroup[VLAN1_BG]
    {
      LIST
      {
        ip =
        {
          adresse = 10.1.0.2
        }
      }
    }
    SELECT vpnBridgeGroup[VLAN2_BG]
    {
      LIST
      {
        ip =
        {
          adresse = 10.2.0.2
        }
      }
    }
  }
action "Activate Configuration"
```

MU-10.10 Utilisation des listes d'accès étendu

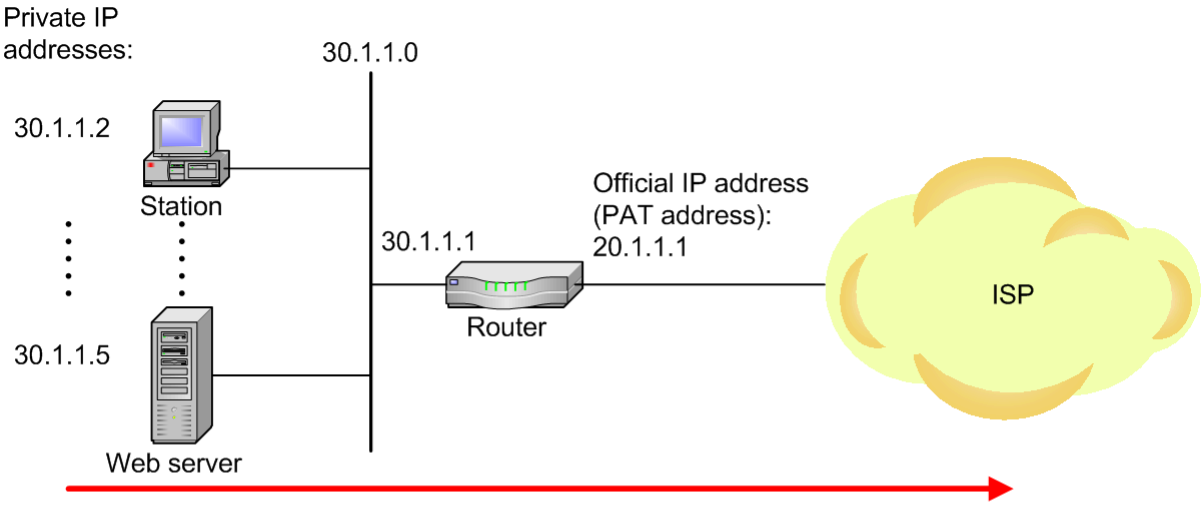
Il s'agit ici d'un exemple de réseau connecté à l'internet et pour lequel les conditions suivantes sont nécessaires:

- seules 5 stations peuvent avoir accès à l'internet.
- seul le port HTTP pour la navigation sur le web est ouvert pour les paquets entrants provenant de l'internet.

La configuration locale est la suivante:

- adresses IP privées:
  - réseau: 30.1.1.0
  - masque net: 255.255.255.0
  - stations: 30.1.1.1 à 30.1.1.5
- adresse IP officielle: 20.1.1.1 (= adresse PAT)

L'adresse de la passerelle de l'ISP est 20.1.1.2.



The access list on the WAN interface (refer to the trafficPolicy[wan] object) filters outgoing traffic. Only the stations with IP addresses 30.1.1.1 up to 30.1.1.5 are allowed to access the Internet.	PAT : the source IP address 30.1.1.x is changed to 20.1.1.1 and the source port is changed to a free port.	To the WAN interface.

To the LAN interface.	The access list on the LAN interface (refer to the trafficPolicy[lan] object) filters incoming traffic. Only port number 80 (www-http) is allowed.

La configuration du Routeur Telindus 1421 SHDSL en format CLI est la suivante:

```
action "Load Default Configuration"
SET
{
  SELECT lanInterface
  {
    LIST
    {
      ip =
      {
        adresse = 30.1.1.1
        trafficPolicy = lan
      }
      mode = routing
    }
  }
  SELECT wanInterface
  {
    LIST
    {
      encapsulation = ppp
    }
    SELECT ppp
    {
      LIST
      {
        ip =
        {
          adresse = 20.1.1.1
          trafficPolicy = wan
          nat = default
        }
        mode = routing
      }
    }
  }
  SELECT router
  {
    LIST
    {
      defaultRoute =
      {
        passerelle = 20.1.1.2
      }
    }
    SELECT defaultNat
    {
      LIST
      {
        patAddress = 20.1.1.1
        servicesAvailable =
        {
          [a] =
          {
            protocol = tcp
            startPort = 80
            serverAddress = 30.1.1.5
          }
        }
      }
    }
    SELECT trafficPolicy[lan]
    {
      LIST
      {
        trafficShaping =
        {
          [a] =
          {
            ipProtocol = TCP
            sourcePortStart = www-http
          }
        }
      }
    }
    SELECT trafficPolicy[wan]
```

```
    {
      LIST
      {
        trafficShaping =
        {
          [a] =
          {
            sourceIpStartAddress = 30.1.1.1
            sourceIpEndAddress = 30.1.1.5
          }
        }
      }
    }
  }
}
action "Activate Configuration"
```

Index

Symbols

<Struct>, qu'est-ce 40

<Table>, qu'est-ce 40

A

acheminement
- activation d'une interface 151
- activités de base 149
- configuration de base 148
- détermination du trajet optimum 149
- introduction 149
- ou pontage 149
- qu'est-ce 149
- statique ou dynamique 153
- transport de paquets 150

acheminement en fonction de la politique
- configuration de base 161
- introduction 162
- qu'est-ce 162

acheminement en fonction de la politique :
- configuration 163

acheminement statique
- configuration de base 152
- introduction 153
- table d'acheminement, configuration 155
- trajet par défaut, configuration 154

action de configuration
- exécution 76
- qu'est-ce 77

action, qu'est-ce 40

activation de la configuration 78

adresses IP
- configuration
  - dans ATM 94
  - dans Frame Relay 114
  - dans PPP 128
  - sur l'interface LAN 62
- configuration de base 52
- explication de la structure IP 55
- gamme privée 187
- imposition sur le côté distant dans PPP 129
- obtention automatique 53
  - dans ATM 93
  - dans Frame Relay 113
  - dans PPP 126
- où trouver les paramètres IP 54

ajout d'un objet dans l'arborescence
- comment 45
- dans (TMA) CLI 45
- dans ATWIN 46
- dans l'interface web 46
- dans TMA 45
- pourquoi 44
- quand 44
- quels objets 44
- référence à l'objet ajouté 47

ajout d'un objet dans l'arborescence 43

applications routeur, introduction 6

arborescence
- ajout d'un objet 43
- de l'unité 41
- qu'est-ce 39
- terminologie 39

ATM
- adresses IP
  - configuration 94
  - obtention automatique 93
- ATM sur G703 104
- configuration de base 84
- Ethernet/IP ponté/acheminé sur ATM (RFC 2684), configuration 100
- introduction 85
- IP classique (IPoA), configuration 101
- PPPoA, configuration 102
- PPPoE, configuration 103
- PVC, configuration 91
- qu'est-ce 85
- UBR, configuration 96
- VPI et VCI, configuration 95

ATM PVC
- configuration 91
- qu'est-ce 85
- redistribution de largeur de bande 97

ATM sur G703
- configuration 104

attribut
- aperçu 48
- qu'est-ce 39

authentification RIP
- activation d'une interface 176
- qu'est-ce 167

avertissement
- EMC 16
- ESD 16
- instructions de sécurité importantes 11
- sécurité 11
- sélection d'un emplacement 13

B

BC
- qu'est-ce 107

BCP
- qu'est-ce 122

BE
- qu'est-ce 107

BECN
qu’est-ce 108
boîtier, ouverture et fermeture 29

C

carte mère, position des commutateurs DIP 27
catégories de service ATM
paramètres de trafic 87
qu’est-ce 87
CCP
qu’est-ce 122
cellules OAM LoopBack (LB), qu'est-ce 90
chaîne binaire, qu'est-ce 40
chaîne d'attributs, lecture vii
CHAP
authentification dans les deux sens 136
authentification dans un sens 135
comment fonctionne 135
configuration 134
qu’est-ce 123
utilisez sysName/sysSecret ou session-Name/sessionSecret? 137
chargement de la configuration par défaut
utilisation de l'action 78
utilisation du commutateur DIP 79
CIR
configuration de base 118
qu’est-ce 107
CLP, qu'est-ce 90
commutateurs à actionnement VLAN par un WAN, exemple de configuration 324
commutateurs DIP 26
aperçu 28
ouverture et fermeture du boîtier 29
position sur la carte mère 27
commutation VLAN
configuration 275
compatibilité avec d’autres unités SHDSL 73
configuration
activation 78
chargement par défaut
utilisation de l'action 78
utilisation du commutateur DIP 79
configuration de base 50
acheminement 148
acheminement en fonction de la politique 161
acheminement statique 152
adresse IP sur l’interface LAN 62
adresses IP 52
ATM 84
CIR et EIR 118
DHCP 253
encapsulation 82
fonctions complémentaires 252
Frame Relay 105
HDLC 144, 145
IPSEC 285
ligne 64
liste d’accès 258
mots de passe 74
OSPF 177
politique de trafic et de priorité sur le routeur 204
politiques, trafic et priorité sur le pont 247
pontage 224
PPP 121
principales fonctions de l’unité 80
QoS 297
RADIUS 291
RIP 166
test d’erreur 146
translation d’adresses 185
tunnel L2TP 278
VLAN 271
configuration de la commutation VLAN 275
connexion avec TMA
par le connecteur de commande 33
par un réseau IP 35
connexion de l'appareil 17
exemple 20
connexion des différentes parties de l’appareil 19
connexion LAN à internet utilisant NAT et PAT, exemple de configuration 315
contrôle de liaison PPP
configuration 130
qu’est-ce 122
conventions utilisées dans ce manuel
graphiques vi
typographiques v
COS, qu'est-ce 207
couches ATM, qu'est-ce 86
couches d'adaptation ATM (AAL), qu'est-ce 86
création de mots de passe dans la table de sécurité 75

D

DE
qu’est-ce 108
déballage 12
déclarations iii
dépistage des erreurs
l'unité 81

DES et 3DES, qu'est-ce 287

DHCP
adresses IP dynamiques, assignation 256
adresses IP statiques, assignation 255
agent relais
configuration de l'unité Telindus comme 257
qu'est-ce 254
configuration de base 253
introduction 254
qu'est-ce 254

Diff-Serv
AF PHB, qu'est-ce 206
Diff-Serv, qu'est-ce 206
PHB, qu'est-ce 206

diffusion dirigée, qu'est-ce 59

DLCI
qu'est-ce 106

DLCI à Frame Relay
configuration 111

document
caractéristiques ii
conventions
graphiques vi
typographiques v
déclarations iii
documentation iv
note sur le copyright ii
organisation iv
public prévu viii
version TDRE décrite dans ce viii
vos réactions viii

documentation iv

E

easy NAT
exemple 202
qu'est-ce 201
que fait 201
quelles sont les conditions 201

EFCI, qu'est-ce 90

EIR
configuration de base 118
qu'est-ce 107

élément, qu'est-ce 40

encapsulation
configuration de base 82
sélection 83

EOC
configuration gestion EOC 67
découverte d'unités sur la ligne SHDSL 68
information récupérée 69
qu'est-ce ? 67

ESP, qu'est-ce 286

Ethernet/IP ponté/acheminé sur ATM (RFC 2684)
configuration 100

exécution des actions de configuration 76

exemple
acheminement en fonction de la politique, configuration 164
commutation VLAN, configuration 277
file par défaut, configuration 221
groupe de pontage, ajout de multiple 240
liste d'accès étendu, configuration 268
NAT, configuration 200
PAT, configuration 190
politique de priorité, application sur une interface 215
politique de priorité, création 214
politique de trafic sur le routeur, configuration 216
politique de trafic, application sur une interface du pont 250
politique de trafic, application sur une interface du routeur 212
politique de trafic, création sur le routeur 211
PPP multiclasses, configuration 143
RIP, configuration 170
trajet par défaut, configuration 154
trajet statique (adresse IP WAN disponible), configuration 156
trajet statique (adresse IP WAN non disponible), configuration 157
tunnel L2TP, configuration 283

exemples 308
combinaison de pontage et d'acheminement dans un réseau 319
connexion d'un LAN à l'internet en utilisant NAT et PAT 315
connexion de commutateurs à activation VLAN par un WAN 324
connexion de deux réseaux par un tunnel 321
extension LAN par un réseau à Frame Relay 311
extension LAN par un réseau ATM 313
extension LAN par un réseau PDH/SDH 309
multiplexage VLAN 326
utilisation de PAT avec un minimum d'adresses IP officielles 317
utilisation des listes d'accès étendu 329

exemples de configuration 308

extension LAN par un réseau à Frame Relay, exemple de configuration 311

extension LAN par un réseau ATM, exemple de configuration 313

extension LAN par un réseau PDH/SDH, exemple de configuration 309

F

FECN
qu’est-ce 108

file d'attente prioritaire, qu'est-ce 205

file par défaut
configuration 219
ou profil de politique de trafic 219
qu’est-ce 219

fonctions complémentaires
configuration de base 252

fragmentation de Frame Relay
activation 120
fragmentation d’interface, qu’est-ce 109
fragmentation de bout en bout, qu’est-ce 109

fragmentation PPP
activation 140
qu’est-ce 125

Frame Relay
adresses IP
configuration 114
obtention automatique 113
adresses IP globales DLCI 115
adresses IP spécifiques DLCI 116
configuration de base 105
DLCI, configuration 111
fragmentation, activation 120
introduction 106
LMI, configuration 117
qu’est-ce 106

G

groupe de pontage
adresse IP, configuration 238
ajout 239
configuration 238
groupes de pontage multiples, qu'est-ce 237
priorité de pontage, réglage 238
protocole de pontage, sélection 238
qu’est-ce 237

groupe, qu'est-ce 40

H

HDLC
configuration de base 144, 145
introduction 145

HMAC MD5 et SHA-1, qu'est-ce 287

I

IEEE 802.1P, qu'est-ce 207

indice, qu’est-ce 39

installation et connexion 10

installation et précautions de connexion 16

instructions de sécurité 11

interface
qu’est-ce ? 51

introduction 4
acheminement 149
acheminement en fonction de la politique 162
acheminement statique 153
applications routeur 6
ATM 85
DHCP 254
Frame Relay 106
HDLC 145
IPSEC 286
l’unité 5
liste d’accès étendu 263
OSPF 178
outils de gestion et de maintenance 7
politiques, trafic et priorité 205
pontage 225
PPP 122
QoS 298
RADIUS 292
RIP 167
terminologie de gestion 37
translation d’adresses 186
tunnel L2TP 279
VLAN 272

IP classique (IPoA), configuration 101

IPCP
qu’est-ce 122

IPSEC
association de sécurité 286
authentification 287
compatibilité 287
configuration d'un tunnel L2TP sécurisé IPSEC 288
configuration de base 285
cryptage 287
encapsulation 287
indice de paramètre de sécurité 287
introduction 286
mode de transport L2TP, qu'est-ce 286
modes 286
puce HWA 290
qu’est-ce 286
services de sécurité 286

L

L2TP pour connecter deux réseaux, exemple de configuration 321

LAC, qu'est-ce 279

LCP
qu’est-ce 122

lecture
chaîne d'attributs vii
tableau de commutateurs DIP vii

ligne
attributs de configuration essentiels 65
compatibilité avec d’autres unités SHDSL 73
configuration de base 64
configuration gestion EOC 67
sécurité d'alimentation, qu'est-ce 73
sélection d'une gamme de vitesse 66
sélection d'une vitesse (gamme) 66
sélection d'une vitesse fixe 66
utilisation d'un répéteur 73
vitesse auto 66
vitesse de ralentissement 66
LIP
qu’est-ce 110
liste d'accès
aperçu 259
liste d'accès étendu
configuration 264
exemple 329
remarques 270
synchronisation 266
liste d’accès
configuration de base 258
liste d’accès étendu
introduction 263
qu’est-ce 263
LMI
configuration 117
qu’est-ce 106
LNS, qu'est-ce 279

M

maintenance de l'unité 30
avec TMA 31
maintenance et gestion
possibilités de connexion 9
MBS, qu'est-ce 87
MLFR
qu’est-ce 110
MLPPP
configuration 138
montage mural 14
mots de passe
configuration de base 74
création dans la table de sécurité 75
entrée dans les différents outils de gestion 75
MPoA
qu’est-ce 89
MS-CHAP
version 1, qu'est-ce 123
version 2, qu'est-ce 124
MS-CHAP, qu'est-ce 123
MTU
qu’est-ce ? 58
multiplexage VLAN, exemple de configuration 326
multi-protocole sur ATM
mécanismes d'encapsulation, qu'est-ce 89
qu’est-ce 89

N

NAT
activation d'une interface 195
ajout de plusieurs objets NAT 197
combinaison avec PAT 201
comment fonctionne 199
easy NAT 201
qu’est-ce 186
quand utiliser 188
NAT sur l’interface LAN, remarque 196
nom d'indice, qu'est-ce 39
nom d’instance, qu’est-ce 39
note sur le copyright ii

O

objet associé, qu'est-ce 39
objet parent, qu'est-ce 39
objet, qu'est-ce 39
organisation de ce manuel iv
OSPF
activation 182
authentification, activation 183
configuration de base 177
introduction 178
qu’est-ce 178
adjacents 180
authentification 181
coût 181
domaine 0 179
domaine d’ossature 179
domaines 179
domaines souches 180
états de liaison 178
liaisons virtuelles 181
routeurs de limite 179
voisins 180
outils de gestion et de maintenance
introduction 7

P

PAP
authentification dans les deux sens 133
authentification dans un sens 132
comment fonctionne 132
configuration 131

qu’est-ce 123
utilisez sysName/sysSecret ou session-Name/sessionSecret? 137

parties de l’appareil 19

PAT
activation d'une interface 189
combinaison avec NAT 201
comment fonctionne 191
limitations et solutions de rechange 194
qu’est-ce 186
quand utiliser 188

PAT avec un minimum d’adresses IP officielles, exemple de configuration 317

PCR, qu'est-ce 87

politique de priorité
application sur une interface 215
création 213
qu’est-ce 205

politique de trafic
application sur une interface du pont 250
application sur une interface du routeur 212
création sur le pont 249
création sur le routeur 210
file par défaut, configuration 219
qu’est-ce 205

politiques sur le routeur
configuration de base 204

politiques, trafic et priorité
configuration sur le pont 248
configuration sur le routeur 209
introduction 205
sur le pont
configuration de base 247
sur les données acheminées et pontées 208

pont à auto-apprentissage, qu'est-ce 227

pontage
activation d'une interface 241
attributs de pontage, présentation 237
configuration 236
configuration d'une interface 242
configuration de base 224
explication de la structure de pontage 243
groupe de pontage, ajout 239
groupe de pontage, configuration 238
introduction 225
ou acheminement 149
qu’est-ce 226

pontage et acheminement dans un réseau, exemple de configuration 319

port de pontage
diagramme de transition d'état 230
etat 230

PPP
adresses IP
configuration 128
imposition sur le côté distant 129
obtention automatique 126
CHAP, configuration 134
CHAP, fonctionnement 135
configuration de base 121
établissement de liaison 122
fragmentation, activation 140
introduction 122
MLPPP, configuration 138
PAP, configuration 131
PAP, fonctionnement 132
PPP multiclasses, configuration 141
qu’est-ce 122
surveillance de liaison, configuration 130

PPP multiclasses
configuration 141
qu’est-ce 125

PPPoA
configuration 102
qu’est-ce 90

PPPoE
configuration 103
qu’est-ce 90

principales fonctions de l’unité, configuration de base du 80

principe de réacheminement, qu'est-ce 160

profil de politique de trafic
ou file par défaut 219

puce 3DES
identification de la version 3DES 290
status 290
version standard ou 3DES 290

puce HWA 290

Q

QoS
configuration de base 297
interface à Frame Relay avec fragmentation 303
interface à Frame Relay multiliaisons avec fragmentation 305
interface à Frame Relay multiliaisons sans fragmentation 304
interface à Frame Relay sans fragmentation 303
interface ATM 306
interface ATM IMA 306
interface Ethernet 300
interface PPP avec fragmentation 301
interface PPP multiliaisons avec fragmentation 302
interface PPP sans fragmentation 301
introduction 298

IP 299
options de fragmentation de Frame Relay 305
qu’est-ce 298
VLAN 300

R

RADIUS
configuration 293
configuration de base 291
introduction 292
qu’est-ce 292
réglages IP
client (appelant) 296
NAS (appelé) 296
types d'attributs supportés 294

réactions viii

redirection ICMP, qu'est-ce 59

référence à un objet ajouté
comment 47
exemple 47
qu’est-ce 47

relais de trame
qu’est-ce 106

remarques concernant
adresse IP sur l’interface LAN en cas de pontage 54, 151, 241, 242
attribut de configuration l2tpTunnels 282
attribut natAddresses 196
attribut rip2Authentication 174
attribut vlanSwitching 276
CIR 118
encapsulation HDLC 145
filtre sur numéros de port 267
fragmentation PPP 140, 141
l'entrée d'alimentation (7,5 / 9 V CC) 19
liste d'accès étendu 270
liste d'accès étendu sur la pile de protocoles 265
politique de trafic de pontage sur l'interface LAN 250
principe de réacheminement 160
sélection d'une gamme de vitesse sur la version 2 paires 66
VLAN sur le LAN et commutation VLAN 272

restriction d'accès
aperçu 259
sur interface IP 259
sur interface pont 260
sur pile de protocoles 261

RIP
activation d'une interface 168
authentification, activation sur une interface 176
comment fonctionne 167
configuration de base 166
explication de la structure RIP 171
introduction 167
qu’est-ce 167
support 167

Router Telindus 1421 SHDSL, qu'est-ce 5

S

SA, qu'est-ce 286

SCR, qu'est-ce 87

sécurité
exigences ii

sélection d'une encapsulation 83

sélection d’un emplacement 13

Spanning Tree
BPDU 232
propagation de 232
qu’est-ce 232
comportement 233
boucles de pontage 233
défaillance de pont 233
extension de réseau 233
coût du trajet, qu'est-ce 234
états des ports de pontage 230
pont racine 228
comment sélectionner 228
qu’est-ce 228
priorité de pont, qu'est-ce 234
priorité de port, qu'est-ce 234
priorité et coût 234
topologie 229

SPI, qu'est-ce 287

structure de pontage
explication 243
où trouver 242

structure IP
explication 55
où trouver 54

structure RIP, explication 171

T

table d'acheminement
configuration 155
règles empiriques lors de la configuration 158

table d’acheminement
qu’est-ce 153

tableau de commutateurs DIP, lecture vii

tag VLAN, qu'est-ce 272

TC
qu’est-ce 108

TDRE
qu’est-ce viii
version viii

témoins DEL 21
diode d’alimentation 23
diode de données de ligne 23
diode de liaison de ligne 23
diode LAN 24
etat 22
introduction 22
terminologie de gestion, introduction 37
test d’erreur
configuration de base 146
TMA
comment connecter 32
connexion par le connecteur de commande 33
connexion par un réseau IP 35
maintenance de l'unité avec 31
qu’est-ce 32
TOS
AF PHB, qu'est-ce 206
champ de précédence, qu'est-ce 206
champ TOS, qu'est-ce 206
DSCP, qu'est-ce 206
octet TOS, qu'est-ce 206
PHB, qu'est-ce 206
trajet par défaut
configuration 154
qu’est-ce 153
translation d'adresses
NAT, activation sur une interface 195
NAT, easy NAT 201
NAT, fonctionnement 199
PAT et NAT, combinaison 201
PAT, activation sur une interface 189
PAT, fonctionnement 191
PAT, limitations et solutions de rechange 194
pourquoi utiliser 186
translation d’adresses
configuration de base 185
introduction 186
NAT, ajout de plusieurs objets NAT 197
qu’est-ce 186
Transparent Spanning Tree, qu'est-ce 227
tunnel L2TP
comment fonctionne 284
configuration 281
configuration de base 278
encapsulation 280
introduction 279
qu’est-ce 279
terminologie 279
type de configuration
active 77
explication 77
non active 77
par défaut 77
qu’est-ce 77

U

UBR
configuration 96
qu’est-ce 88

V

valeur complexe, qu'est-ce 40
valeur d’instance, qu’est-ce 39
valeur structurée, qu'est-ce 40
valeur, qu'est-ce 39
VCI
configuration 95
qu’est-ce 85
VLAN
configuration 273
configuration de base 271
introduction 272
qu’est-ce 272
VPI
configuration 95
qu’est-ce 85
vue arrière de l’appareil 18